QP CODE: SSC/Q0903
QP TITLE: Analyst Application Security

OVERVIEW

Test Duration	190 minutes
Natural Language Options	English
Distribution of Marks	As mentioned in the Qualification Pack
Pass Criteria	70% in each NOS (on Moderated Score)
Technology tools / Platforms Tested (Mandatory)	
i) Web Crawlers	ii) Bugtraq
iii) Shell Script	iv) Java Script
Technology tools / Platforms Tested (Select any one)	
Infrastructure Requirements	As per standard list provided to Assessment Centers
QP Specific Infrastructure Requirements (if any)	
i)	ii)

SAMPLE QUESTIONS

SECTION 1/ NOS SSC/N0909 (Identify exposures and weaknesses in applications and their deployments)

1.

Statement: Which of the following type of security application will help you secure the network by granting only security policy–compliant devices access to network assets?

Options:

- **A.** Firewall
- **B.** Antivirus
- **C.** Network Access Control
- **D.** Intrusion Detection System

Correct Answer: C. Network Access Control

2.

Statement: You receive a call from an unknown caller who starts inquiring about your company and attempts to ask about some of the confidential information. What form of information gathering is the person trying?

Options:

- **A.** Dumpster Diving
- **B.** Social Engineering
- **C.** Zero-day exploit
- **D.** None of the given options

Correct Answer: B. Social Engineering

3.

Statement: You have been asked to perform a test to find the misconfigurations of the existing network. Which of the following method should help you achieve this goal?

Options:

- **A.** Vulnerability Scan

- **B.** Penetration Test
- **C.** Code Review
- **D.** Brute Force Scan

Correct Answer: A. Vulnerability Scan

4.

Statement: You have been receiving unsolicited messages on your mobile phone. Which of the following method is being used by the attacker?

- **A.** Bluejacking
- **B.** Man-in-the-middle
- **C.** Packet Sniffing
- **D.** XSRF

Correct Answer: A. Bluejacking

5.

Statement: If a software development organization owns a Vulnerability Database (VDB), who is likely to be the user of this database?

Options:

- **A.** Auditors
- **B.** Administrators
- **C.** Hackers
- **D.** All of the given options

Correct Answer: D. All of the given options

6.

Statement: You are testing an application for invalid input acceptance and semi-malformed data injection. Which type of testing are you doing?

Options:

- **A.** Brute-force
- **B.** Vulnerability scan

C. Penetration testing
D. Fuzzing

Correct Answer: D. Fuzzing

7.

Statement: You have discovered a vulnerability, but you suspect this vulnerability might be known. Which would be the best place to check for this known or unknown vulnerability?

Options:

A. Common Vulnerabilities and Exposures (CVE) Website
B. A public Website
C. A hacker forum
D. All of the given options

Correct Answer: D. All of the given options

SECTION 2/ NOS SSC/N0910 (Harden application and deployment configurations for minimizing exposure and vulnerabilities)

8.

Statement: You have an application server. You regularly update the operating system with the latest updates. However, applications on the server are not updated with latest software updates. If you want to mitigate risks on the applications of this server, what would be your best strategy?

Options:

A. Configure a firewall on the server and allow restricted access to the application
B. Perform application hardening using an automated tool
C. Configure a patch management system to regularly apply patches
D. Configure logging on the application to track users who access it

Correct Answer: C. Configure a patch management system to regularly apply patches

9.

Statement: You are validating a server that was hardened a few months back. After the validation against the baseline documentation, you find that the server has an outdated application. What should be your immediate step?

Options:

A. Remove the outdated application
B. Update the documentation
C. Upgrade the application with a new version
D. All of the given options

Correct Answer: A. Remove the outdated application

10.

Statement: Identify the methods indicating that your Web application is hacked.

Options:

A. Unexpected log messages
B. Discovery of new processes and services
C. Discovery of new and unwanted files
D. All of the given options

Correct Answer: D. All of the given options

11.

Statement: To be able to implement the patch management process in proper order, sequence the steps in correct order:

1. Detect
2. Assess
3. Acquire
4. Test
5. Deploy
6. Maintain

Options:

A. 1, 2, 3, 4, 5 and 6
B. 1, 4, 2, 3, 5 and 6

C. 3, 1, 2, 4, 5 and 6

D. 2, 1, 3, 4, 5 and 6

Correct Answer: A. 1, 2, 3, 4, 5 and 6

12.

Statement: You have been asked to implement a patch management technology that can meet the following goals:

1. **Support remote hosts**
2. **Support managed hosts**
3. **Requires minimal bandwidth for scanning**
4. **Can detect a large number of applications**

To meet this required goal, which of the following technology should you implement?

Options:

A. Agent-Based

B. Agentless Scanning

C. Passive Network Monitoring

D. All of the given options

Correct Answer: A. Agent-Based

SECTION 3/ NOS SSC/N0911 (Monitor applications and solutions deployed for possible breaches and compromises)

13.

Statement: If you are using an open WIFI connection at the airport, which of the tools can an attacker use to eavesdrop on emails or copy passwords as they pass over the network?

Options:

A. Ettercap

B. Wireshark

C. Cain and Abel

D. All of the given options

Correct Answer: D. All of the given options

14.

Statement: Which of the following should you use to monitor a specific server containing critical data?

Options:

A. HIDS
B. HIPS
C. NIPS
D. NIDS

Correct Answer: A. HIDS

15.

Statement: Your organization has an open Bring Your Own Device (BOYD) policy. You, as the CISO, wants to ensure that even if the BOYD device is stolen, the information on it is still safe. Identify the correct methods that you should implement:

1. Screen locks
2. Geo-tracking
3. Asset tracking
4. Device encryption

Options:

A. 1 and 4
B. 2 and 4
C. 3 and 4
D. 2 and 3

Correct Answer: C. 3 and 4

16.

Statement: **One of your Web server has been recently compromised. You review the firewall logs and find that a number of ports and protocols have been recently used. You notice the following ports in the logs:**

22, 25, 443, 445, 1445, 3389

If you were the security analyst to investigate this attack on the Webserver, which protocol do you think has been used in the attack?

Options:

A. LDAP
B. SSH
C. RDP
D. SMTP

Correct Answer: B. SSH

17.

Statement: If you are building an incident management system, which of the following task are you performing in the National Initiative for Cybersecurity Framework?

Options:

A. Operate and Maintain
B. Protect and Defend
C. Oversee and Govern
D. Collect and Operate

Correct Answer: B. Protect and Defend

SECTION 4/ NOS SSC/N9001 (Manage your work to meet requirements)

18.

Statement: As you begin your day's work, which of the following should you take from the line manager regarding your work?

Options:

A. Names of the customers whose requests must be processed
B. Work schedule and requirements for the day
C. List of equipment to be used for that day
D. Timings of tea and lunch break

Correct Answer, B. Work schedule and requirements for the day

19.

Statement: While resolving customer issues, you must refer to many manuals and policy books. Which of the following is a good place to store all this reference material?

Options:

A. Right there on the desk for easy access
B. Organize around the desk storage
C. In the company's library
D. Line them on the overhead shelf in a logical order

Correct Answer, D. Line them on the overhead shelf in a logical order

20.

Statement: You are in a meeting about economizing office resources and the host of the meeting invites suggestions from those present. Which of the following is not a viable suggestion?

Options:

A. Waste printouts should be used for creating notepads for internal use
B. Computers should be on automatic standby mode
C. Air conditioning units should be maintained at ideal temperatures
D. Computers should be shut down every time a person leaves his/her desk

Correct Answer, D. Computers should be shut down every time a person leaves his/her desk

21.

Statement: A customer asks a technical detail regarding Radmin, which you are not aware of. What will you do in such a situation?

Options:

A. Tell the customer it is not possible for you to disclose
B. Discuss the situation with your line manager
C. Ask a subject matter expert for the answer
D. Put the phone down

Correct Answer, C. Ask a subject matter expert for the answer

22.

Statement: Which of the following is an example of a day end report to be submitted to the line manager?

Options:

A. Summary of cases handled, actions taken and statuses
B. Complete hour by hour accounting of your time in office
C. Complete list of calls that you attended
D. Summary of the cases which were closed successfully

Correct Answer, A. Summary of cases handled, actions taken and statuses

SECTION 5/NOS SSC/N9002 (Work effectively with colleagues)

23.

Statement: Which of the following should you keep in mind when communicating with your colleagues?

Options:

A. Stating the issue clearly
B. Giving concise information
C. Providing accurate details
D. All the given options

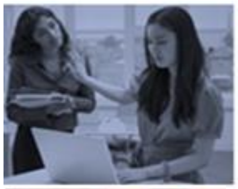
Correct Answer, **D.** All the given options

24.

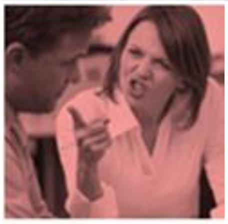
Statement: Which of the following is the correct way to respond to a colleague asking for your assistance?

Options:

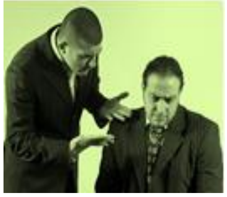
A.



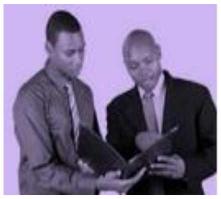
B.



C.



D.



Correct Answer, D**.**

25.

Statement: You have committed to provide the logs of a case to your colleague by EOD. However, due to some unavoidable circumstances you have not been able to do that. What should you do?

Options:

A. Ignore the customer
B. Tell your colleague falsely that the deadline was some other date
C. Apologize to him/her and complete the task as soon as possible
D. Blame your colleague for giving the task on such a short notice

Correct Answer: C. Apologize to him/her and complete the task as soon as possible

26.

Statement: Due to a personal emergency, you need to suddenly leave office in the middle of on an ongoing escalation of an issue. What should you do?

Options:

A. Inform that you will not be able to resolve the issue that day
B. Leave the task for the next day
C. Call your supervisor for any progress update
D. Inform your supervisor and request him to hand over the issue to a colleague

Correct Answer, D. Inform your supervisor and request him to hand over the issue to a colleague

27.

Statement: A newly joined colleague is facing difficulty in resolving technical problems of customers. What should you do in such a situation?

Options:

A. Offer to guide him/her with basic troubleshooting techniques
B. Ask him/her to observe carefully when a senior colleague solves a tricky issue
C. Both A & B
D. None of the given options

Correct Answer, C. Both A & B

SECTION 6/NOS SSC/ N9003 (Maintain a healthy, safe and secure working environment)

28.

Statement: You are down with flu but must complete an important task at the office the next day. What should you do?

Options:

A. Come to office, finish your task and leave early
B. Come to office and ask your co-worker for help
C. Take leave without informing anyone
D. Inform your supervisor and take leave as flu is contagious

Correct Answer, D**.** Inform your supervisor and take a leave as flu is contagious

29.

Statement: You notice that a co-worker has been letting in visitors inside the office building without filling any visitor's information details. What should you do?

Options:

A. Do not do anything as there is no danger from personal visitors
B. Request the co-worker to fill the visitor's information detail
C. Inform the security in-charge about non-compliance of the company's security procedure
D. Inform the supervisor

Correct Answer, C**.** Inform the security in-charge about non-compliance of the company's security procedure

30.

Statement: You notice that the stairs in the office building are not properly lit which could lead to accidents. What should you do?

Options:

A. Inform your supervisor
B. Ignore the issue as people use elevators and not stairs
C. Not do anything as this is not your responsibility
D. Inform the maintenance department and also warn your co-workers

Correct Answer, D. Inform the maintenance department and also warn your co-workers

31.

Statement: What should you do if you see an intruder behaving suspiciously in the office?

Options:

- **A.** Call the security in-charge and give him complete information
- **B.** Physically confront the person
- **C.** Block the person's access to an exit
- **D.** Raise an alarm and warn your co-workers

Correct Answer, A. Call the security in-charge and give him complete information

SECTION 7/NOS SSC/ N9004 (Provide data/information in standard formats)

32.

Statement: Whom should you consult with, if you want to know the daily report submission timeline?

Options:

- **A.** Supervisor
- **B.** Colleagues
- **C.** Any employee
- **D.** Any team member

Correct Answer, A. Supervisor

33.

Statement: A customer asks you about technical specifications of your company's third-party software, but you do not have the exact knowledge. In which order, will you take the following steps to get correct information to give to the customer?

A. Take detailed specifications from the subject matter expert

B. Ask a senior colleague with troubleshooting experience in that software

C. Discuss the issue with your manager

Options:

A. A--> B --> C

B. B --> C--> A

C. A --> C --> B

D. B -->A--> C

Correct Answer, B. B --> C--> A

34.

Statement: A fault occurs in a secure category product of the company. How should you handle it?

Options:

A. Ask your manager's permission to solve the problem
B. Ask your manager to assign it to a senior colleague
C. Ask a subject matter expert to help you in solving the problem
D. Forward it to the specific team certified in operation and maintenance of secured products

Correct Answer, D. Forward it to the specific team certified in operation and maintenance of secured products

35.

Statement: Which of the following categories require an in-depth analysis of data before it is shared with the client?

Options:

A. Data collection
B. Data extraction
C. Data privacy
D. None of the given options

Correct Answer, B. Data extraction

36.

Statement: Which of the following problems should you report to your manager?

Options:

A. Incorrect reporting of problem
B. Incorrect detection of type of problem
C. Incorrect solution of problem
D. All the given options

Correct Answer, D**.** All the given options

SECTION 8/NOS SSC/N9005 (Develop your knowledge, skills and competence)

37.

Statement: You need to learn manual security tools such as Paros Proxy and HttpWatch. Which of the following people can help you in such a scenario?

Options:

A. Your QA Manager
B. Your team members
C. Professionals of these tools
D. All the given options

Correct Answer, D**.** All the given options

38.

Statement: Arrange the following steps that you will take to find out the competency development needs in relation to your role in the correct order.

A. Assessment by Manager and Subject matter expert
B. Self-Assessment through Competency Assessment Tool
C. Internal Certifications

Options:

A. A --> B --> C
B. B -->A--> C
C. B -->C-->A
D. A --> C --> B

Correct Answer, B. B -->A--> C

39.

Statement: While working on a project module with critical timelines, you feel stressed and are unable to work efficiently. Identify the knowledge and skills you should learn to handle such situations.

Options:

A. Knowledge of the practical application of engineering science and technology related to your project
B. Business Communication skills and Interpersonal skills
C. Behavioral skills such as Time management, Stress management and Goal setting
D. Leadership skills

Correct Answer, C. Behavioral skills such as Time management, Stress management and Goal setting

40.

Statement: You have designed a plan to develop your competency in IP domain. Which of the following certifications is applicable to you?

Options:

A. Cisco Certified Network Associate
B. Microsoft Certified Network Associate
C. Oracle Certification
D. SAP Certification

Correct Answer, A. Cisco Certified Network Associate