2025

BRICS SKILLS COMPETITION

(BRICS+ FUTURE SKILLS & TECH CHALLENGE)

Cyber Security

BRICS-FS-28

Test Project
(International Finals_Online)

September 2025

Catalogue

1. Form of participation 1

2. Competition contents 1

3. Competition stage and time requirements 1

4. Task definition 2

4.1. Sample first stage 2

4.2. Sample second stage 4

4.2.1. Task description 1 4

4.2.2. Example answer 5

4.2.3. Task description II 5

4.2.4. Example answer 6

4.3. Sample third stage 6

4.3.1. Task description 1 6

4.3.2. Example answer 6

4.3.3. Task description 2 7

4.3.4. Example answer 7

4.4. Sample test for stage 4 8

4.4.1. task description 8

4.4.2. Example answer 9

1. Form of participation

The cyber Security event of the BRICS Skills Competition 2025 (BRICS Future Skills and Technology Challenge) will be held in a two-person competition.

2. competition contents

The competition consists of four stages, as shown in the following table:

order number	content of examination
stage Ⅰ	Professional quality and theoretical skills
stage Ⅱ	Application of network and data security skills
phase III	Application of network security operation skills
Phase IV	Cyber security challenges arising from new technologies and new areas of application (Trusted Data Space Security)

Only when the competition tasks and scoring criteria cannot be completed on-site and have been approved by the chief expert may any modifications be made. Participants who fail to comply with occupational health and safety regulations, or put themselves and others at risk, may face disqualification. After completing all stages, the results will be scored.

3. Competition stage and time requirements

The network security competition consists of four stages, which require the

contestants to complete them within the specified time. The specific stage names and time requirements are as follows:

order number	Stage assessment content	Duration of the match (minutes)
stage Ⅰ	Professional quality and theoretical skills	60
stage Ⅱ	Application of network and data security skills	90
phase III	Application of network security operation skills	90
Phase IV	Cyber security challenges arising from new technologies and new areas of application (Trusted Data Space Security)	60

4. task definition

4.1. Sample first stage

1. Which of the following is not part of the professional qualities that a contestant should have? ()

A. Awareness of cybersecurity norms

B. Strict observance of work and competition discipline

C. Proactive risk prevention

D. Omission of time nodes in the mandate

2. Which of the following is not a common Web vulnerability? ()

A.SQL pour into

B. Cross-site scripting (XSS)

C. Cross-site request forgery (CSRF)

D. Port scanning

3. The three basic attributes of data security are ().

A. Confidentiality, integrity and availability

B. Confidentiality, timeliness and availability

C. Reliability, integrity and availability

D. Confidentiality, integrity and scalability

4. In the emergency response process, which of the following is not a common troubleshooting item? ()

A. Account screening

B. Network communications and port troubleshooting

C. System backdoor detection

D. System hardware specification troubleshooting

5. In Windows system, which of the following is a strong password policy setting requirement? ()

A. Password length is at least 3 digits

B. Password can contain username

C. The password must contain three categories of uppercase letters, lowercase letters, numbers and special characters

D. Passwords can be changed for a long time

6. In Linux system, the command used to check the empty port password user is ().

A. cat /etc/shadow | awk -F: '$2 == "" {print $1}'

B. ls -l /etc/passwd

C. net user

D. chkconfig --list

7. Which of the following is not part of data lifecycle management? ()

A. Data creation

B. data storage

C. Data destruction

D. Data cloning

8. In emergency response, the common method to identify Webshell files is ().

A. Check document creation time

B. Analysis of content signatures (e.g., suspicious code)

C. Viewing file size

D. Judging by file extensions

9. Which of the following is the main regulatory object of the Regulations on the Security Protection of Critical Information Infrastructure? ()

A. General corporate websites

B. personal blog

C. Operators of critical information infrastructure

D. Social media accounts

4.2. Sample second stage

4.2.1. Task description 1

As a cybersecurity researcher, you discovered a potential SQL injection vulnerability in the login system of an online bookstore called "Sea of Knowledge".

The user data (including usernames and passwords) is stored in a database table named users. Your task is to exploit this vulnerability to obtain the administrator account credentials.

4.2.2. Example answer

- First, try to enter 'OR 1' = '1' and any value into the user name and password input boxes of the login page respectively, and observe whether the page returns abnormal or error information to verify whether there is an SQL injection vulnerability.
- If there is a vulnerability, construct the query statement 'UNION SELECT username,password FROM users WHERE username=' admin 'to obtain the administrator account's username and password.
- After obtaining the administrator's username and password, use these credentials to log in to the background management system, find the files or pages containing sensitive information, and extract the hidden flag (e.g., flag{admin_password_is_123456}).

4.2.3. Task description II

During a security assessment of a company's email server, you intercepted a network communication containing an encrypted attachment. The file is suspected to contain sensitive information such as employee payroll records or confidential corporate contracts. Your task is to analyze the data packet, extract the attachment, and decrypt its contents.

4.2.4. Example answer

- Use Wireshark or other network analysis tools to open the provided.pcap file and look for traffic related to email transmission (e.g., packets from SMTP or IMAP protocols).
- Extract the encrypted attachment content from the data packet in the email attachment. Note that the attachment may use Base64 or hexadecimal encoding.
- Analyze the file header information in the attachment to determine the encryption algorithm (such as AES or RSA).
- Based on the problem prompt, try to use a common encryption key (such as password123 or flag{}) to decrypt. For example, if the attachment is AES encrypted, you can try to use an AES tool or Python script to decrypt it.
- After decryption, find the hidden flag, such as flag{sensitive_data_leakage Detected}.

4.3. Sample third stage

4.3.1. Task description 1

There are many employee computers in the office network of the company. One day, the network administrator found abnormal network traffic and some employee computers had blue screen phenomenon. It is suspected that there is malicious software spreading in the Intranet, so you need to investigate and deal with it.

4.3.2. Example answer

- Intrusion detection: Analyze memory swap files to identify suspicious processes

and services, such as unknown network connections or malware signatures. Examine network traffic statistics to detect abnormal IP addresses that could indicate infected devices or attack sources.

- Inhibit disposal: Isolate infected computers in the network to prevent further spread of malware.
- Terminate suspicious processes found in memory to prevent malware from running.
- System recovery: Perform virus scanning and removal on infected computers, and use security software to eliminate malware.
- Restore affected system files and services to ensure proper computer operation.
- Evidence collection: Extract malware samples and related network information from memory files as evidence for investigation.
- Record the IP address of the infected computer, the time of infection and symptoms.

4.3.3. Task description 2

The company's cloud platform server was attacked and some data was stolen. You need to analyze the logs and network traffic of the cloud platform, find out the source and path of the attack, and propose security reinforcement plans.

4.3.4. Example answer

- Traceability analysis: Analyze the access logs of cloud platform servers to find abnormal login records, API call records, etc., and determine how the attacker enters the system.

- Check the network traffic data to identify the source IP of incoming traffic and the target IP of outgoing traffic related to the attack, and track the path of data leakage.
- Security reinforcement: According to the results of traceability analysis, access control of the cloud platform is strengthened, such as restricting IP access whitelist and strengthening identity authentication.
- Update the security policy of the cloud platform, close unnecessary ports and services, and reduce the attack surface.
- Update the patch of the cloud platform server to fix known security vulnerabilities.
- Tracking the attack path: Through the correlation analysis of logs and network traffic, restore the complete process of the attacker from intrusion to data theft, including the use of attack tools and methods.

4.4. Sample test for stage 4

4.4.1. task description

Yesterday, Company A's intrusion detection system flagged a malicious horse virus attack on its website. To trace the hacking trail, the company exported relevant data packets from the security system. As a cybersecurity specialist, I assisted the company in analyzing these data packets (named hack.pcap) to identify and resolve the following critical issues:

- First question: What is the user name and password used by hackers to log in to the unit's website? (Submit format: account/password, answer example: admin/123456)

- Second question: What is the name of the webshell file written into the server after a hacker breaks into the website of an organization? (Please include the file extension when entering the answer. For example: webshell.txt)

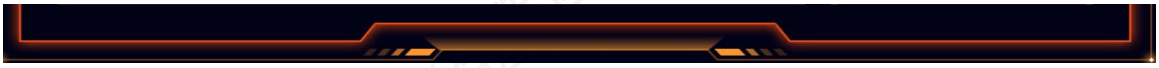
4.4.2. Example answer

Open hack.pcap with wireshark, find the hacker's login username and password in tcp.stream eq 6, and the server responds with 200

We can find that the user name is test, and decrypt the password via URL to get Admin123!@#. Therefore, the final answer to the first question is test/Admin123!@#. Submit this answer to the platform with the title: 1-1webshell in the input box and click submit

Answer correctly The platform will inform and receive the score for that question (if correct)

If the answer is wrong, the platform will inform you and deduct your chance to answer (if the answer is wrong)



Note: If the command returns an error result as shown in the figure, it means that the question has not been completed. Then there is no score for this question!