BRICS
2022 CHINA

TEST PROJECT

BRICS-FS-28_Cyber Security

2022 BRICS Skills Competition

2022 BRICS Skills Competition

Cyber Security

Sample Project

The project includes the following sections:

1. The form of the competition
2. Project stage brief introduction
3. Project phase and time required

Assigned time to complete the task: 12 hours.

I. The form of the competition

Team participation, 3 players from each team (1 captain).

II. Introduction to the project stage

The project consists of four phases and will be completed sequentially.

Provide participants with instructions for answering questions, target machine information, IP address assignment form and message address assignment form.

Projects include installation and commissioning based on system integration, network deployment, and cloud computing processing:

1. Professional quality and theoretical skills
2. Safe operation
3. Emergency response
4. CTF Capture the Flag

Project phases and standards can only be changed if the competition environment cannot be completed and is approved by the Skills Competition Manager.

Competitors may be removed from the competition if they fail to comply or put themselves and / or other competitors at risk.

Phase items will be completed in order according to a random draw.Results will be scored when the participants complete the module.

III. Project phase and time required

1.Stage and time summary

Order number	Stage name	Stage completion time
1	Stage 1: Professional quality and theoretical skills	90 Minutes
2	Stage 2: safe operation	210 Minutes
3	Stage 3: Emergency response	210 Minutes
4	Stage 4:, CTF captures the flag	210 Minutes

Table 1 Project stage list

2. Schedule of events (draft)

Date	Work plan (Beijing Time)	Matters	Description of the job content	Remark
In 2022	Beijing Time 7:30-8:00	Check-in, record and report of the participants	All the players	The day of the competition
	Beijing Time 8:00-8:30	The contestants draw lots, one encryption	captain	
	Beijing Time 8:30-9:00	Contestants draw lots, the second encryption	All the players	
	Beijing Time 9:00-9:30	Admission, reading room discipline, Check and confirm the PC problems	Participants, the referee group, the supervision and arbitration group	
	Beijing Time 9:30-10:00	Check the distribution of environmental competition questions	Participants, the referee group, the supervision and arbitration group	
	Beijing Time 10:00-11:30	Team competition	All the players	
	Beijing Time 11:30-12:30	Lunch time for the participating teams	All the players	
	Beijing Time 12:30-16:00	Team competition	All the players	
In 2022	Beijing Time	Check and report the participants	captain	The next day of the

	7:00-7:30			competition
	Beijing Time 7:30-8:00	The contestants draw lots, one encryption	All the players	
	Beijing Time 8:00-8:30	Contestants draw lots, the second encryption	Participants, the referee group, the supervision and arbitration group	
	Beijing Time 8:30-9:00	Admission, reading room discipline,	All the players	
	Beijing Time 9:00-12:30	Check and confirm the PC problems	All the players	
	Beijing Time 12:30-13:30	Team competition	Expert group, referee group	
	Beijing Time 13:30-17:00	Lunch time for the participating teams	Leaders, guests, the referee group, each participating team	
	Beijing Time 17:00-24:00	Team competition	All the players	
In 2022	Beijing Time 9:00-11:00	Expert referee score	captain	One day after the competition

Table 2 Event Process Plan

Sample Title

StageI: Professional quality and theoretical skills

Background: As an information security technician must be able to master the foundation of the operating system, network foundation, database foundation and other relevant basic knowledge, and use these basic knowledge to further learn the information security technology to master fuzzy testing, vulnerability mining, so as to have the foundation to become a high-level information security personnel.

The topics in the theoretical stage mainly include professional quality, network security, safe operation, emergency response and other related contents. The details are shown in the following table:

Order number	**Content module**	**Explain**
Stage I (theory)	Professional quality	Network security standard consciousness, security consciousness, discipline consciousness;
	Network security	Router, switch, firewall, log audit, intrusion detection and other security network security equipment management and security configuration; Firewall routing, security policy, NAT, VPN and other configuration and testing; Network log system network detection, statistics, alarm and other configuration; The web application of firewall protection policy, filtering policy, alarm and other configuration; Wireless management, wireless network setting, security policy and other configuration and testing; Three-layer switch routing, second-floor security and other configuration and testing;

	Safe operation	Windows Server system and Linux system safety operation knowledge point assessment;
	Emergency response	Operating system and application system of log analysis, vulnerability analysis, system process analysis, memory analysis, system security reinforcement, program reverse analysis, coding conversion, encryption and decryption technology, data steganography, file analysis, network traffic package analysis, mobile application analysis, code audit and other commonly used penetration and protection management knowledge assessment;

Project 1 professional quality

1. Which of the following commands will cause fatal damage to the Linux system

   A. rm -f *

   B. rm /tmp

   C. yum update

   D. cat /dev/null > /etc/fstab

2. What are the main contents of key management?

   A. Generate, assign, use, store, backup, restore, and destroy

   B. Generate, examine,, use, store, backup, restore, and destroy

   C. Generate, assign, use, download, backup, restore, and destroy

   D. Generate, verify, use, store, backup, restore, and destroy

3. The following is the correct description of the regular encryption key distribution scheme?

   A. Reduce costs with disaster recovery

   B. Provide sufficient capacity to meet the business needs

   C. Provide reasonable guarantees to satisfy the liability to the customer

   D. Generate performance reports in time

4. What is the correct command to view the certificate information using the openssl tool?

   A. openssl x509 -noout -text -in cert .pem

   B. openssl x509 -noout -text -key cert .pem

   C. openssl genrsa -noout -text -in cert .pem

   D. openssl cert -noout -text -in cert .pem

5. The default parameters that you can view when generating certificates with cfssl are correct?

   A. config,pem

   B. c onfig,csr

C. csr,pem

D. csr,configs

6. Which of the following is the greatest risk when storage growth on a critical file server is not properly managed?

   A. Backup time will grow steadily

   B. Backup costs can grow rapidly

   C. Storage costs can grow rapidly

   D. The server recovery work does not meet the recovery time target (RTO) requirements

7. In the CMM criteria, which level indicates that the organization has established quantitative quality indicators during software development?

   A. Repeatable level

   B. Definition level

   C. Managed level

   D. Optimized level

8. Which of the following tests is the most effective in order to let in-program interface errors be detected early during software development?

   A. bottom-up testing

   B. white box testing

   C. top-down testing

   D. black-box testing

9. In the Trusted Computer System Assessment Guidelines (TCSEC), which of the following is the lowest level to meet the mandatory protection requirements?

   A. C2

   B. C1

   C. B2

   D. B1

10. The Clark-Wilson model can meet all three integrity security objectives, and which one is wrong?

A. Prevent inappropriate modifications by authorized users

B. Prevent unauthorized users from tampering

C. Maintain both internal and external consistency

D. Ensure data and procedures

11. Which command in a linux system can you view files and directories and display the properties of files?

A. cat

B. mkdir

C. ls

D. ls –l

12. Which command is used for a disk partition in a linux system?

A. parted

B. mv

C. du

D. df

13. Which of the following is the most important consideration when implementing the IT governance?

A. Process maturity

B. performance index

C. venture

D. Guarantee report

14. Which of the following measures is not a Login access control measure?

A. Audit the login person information

B. Password failure time

C. Password length

D. Login failure number limit

15. Which of the following items is being specifically used for user identification?

A. PIN

B. phone code

C. IP address

D. MAC address

Project 2 network security

16. Which of the following Data Backup methods is the fastest in time?

A. Incremental Data, Backup

B. Differences Data, Backup

C. Totally Data, Backup

D. disk mirroring

17. Which of the following is not a Electromagnetic radiation leakage protection method?

A. Red and black power supply

B. Shield machine room

C. Video distractor

D. Anti-static clothing

18. Which of the following malicious programs can spread autonomously without touching any media?

A. cockhorse

B. virus

C. worm

D. Fishing program

19. The following devices are commonly used for risk analysis?

A. Firewall

B. IDS

C. Vulnerability scanner

D. UTM

20. The registry running command for the Windows operating system is:

    A. Regsvr32

    B. Regegit

    C. Regedit.msc

    D. Regedit.mmc

21. Create the DNS main area when installing the active directory. The area record exception causes the directory service. You can rewrite the DNS area by restart Windows's ()?

    A. Server serve

    B. The NetLogon Services

    C. The Messenger Services

    D. The NetworkDDE Services

22. Turning off Windows Network Sharing requires the () service?

    A. Server

    B. Workstation

    C. ServiceLayer

    D. Terminal Services

23. Group policies in AD cannot be applied to?

    A. land within certain boundaries

    B. OU

    C. site

    D. group

24. The encryption technology used by the EFS encryption file system is the ().

    A. DES

    B. 3DES

    C. IDEA

D. RSA

25. Which of the following IDS is most likely to generate false alerts to normal network activity?

A. Based on statistics

B. Based on the digital Signature's

C. neural network

D. Based on the host

26. A long-term employee, with a strong technical background and management experience, applies for a position in the audit department. Should he be hired based on his personal experience and ____?

A. Length of years of service, as this will help to ensure the technical capability.

B. Age, (if too old), may be impractical in auditing technology training.

C. Information system knowledge, because this will strengthen the credibility of the audit

D. Capability, as an information system auditor, will be independent of existing information systems

27. One organization uses an ERP, and which of the following is an effective access control?

A. User-level permissions

B. Based on the role

C. fine grain

D. discretionary access control

28. Which of the following is effective in preventing CC attacks?

A. Delete a page with a possible CC attack

B. Improve the server performance

C. Limit the number of visits per second that individual IP addresses can access the server

D. Use the IDS devices

29. The following is the most accurate statement for Windows host security

A. Safest possible after system reinstallation

B. The system is safe with antivirus and Firewall installed

C. The administrator password length modification is more complex security

D. The professional security service personnel evaluates according to the needs of the business system, and then compare the safety reinforcement according to the evaluation results

30. Which of the following security mechanisms is an abstraction machine that does not only ensure that the subject has the necessary access rights, but also ensures that there is no unauthorized access and disruptive modifications to the object?

A. security kernel

B. trusted computing base

C. Reference monitor

D. margin of safety

31. Is is correct about the basic elements involved in security audit?

A. Security audit can be divided into real-time intrusion security audit and post-audit detection

B. The basic elements of safety audit are control objectives, security loopholes, control measures and control tests

C. The basic elements of safety audit are the control target, security loopholes, control measures and detection

D. Safety audit can be divided into control measures and detection control

32. Here is the most complete description of the security audits?

A. The security audit system can audit all the plaintext data

B. Security audits can only audit the website system

C. Security audits can audit the database

D. Security audit can audit website forums

33. When a company performs a disaster recovery test, Information security professionals noticed that the server at the disaster recovery site is slow. In order to find the root cause, he should first check:

A. Error event report for the disaster recovery site

B. The Disaster Recovery Test Plan

C. Disaster Recovery Plan (DRP)

D. Profile for the primary site and disaster recovery sites

34. To meet the organizational disaster recovery requirements, the backup time intervals must not exceed:

A. Service Level Objective (SLO)

B. Recovery Time Target (RTO)

C. Restore point Target (RPO)

D. Maximum acceptance of withdrawal (MAO)

35. Which of the following questions in an IT system disaster recovery test should be the most concerned?

A. Due to the limited test time window, only the most necessary systems were tested, and the other systems were tested separately for the rest of the year

B. During testing, some backup systems are defective or not functional, resulting in testing of these systems to fail

C. The process of closing and protecting the original production site before opening a backup site takes much more time than planned

D. This test is performed by the same staff every year, and no Disaster Recovery Plan (DRP) documentation is used because all participants are familiar with each recovery step

Project 3 Safe operation

36. Which aspect of security does the Bell-LaPadula security model focus on?

A. Auditable

B. integrity

C. confidentiality

D. serviceability

37. Which of the following control models is implemented based on security tags?

A. discretionary access control

B. mandatory access control

C. Rule-based access control

D. Identity-based access control

38. Which of the following roles is responsible for the data security?

A. Data owners

B. Data regulators

C. user

D. safety manager

39. The security weakness of the system itself, that can be exploited by hackers, is called?

A. vulnerability

B. risk

C. threaten

D. weakness

40. The possibility that the system's weaknesses are exploited by hackers is called?

A. risk

B. Residual risk

C. expose

D. odds

41. Which of the following accurately describes a trusted calculation basis (TCB)?

A. TCB only on firmware (Firmware)

B. The TCB describes the level of security provided by a system

C. The TCB describes a protective mechanism within a system

D. The TCB represents the sensitivity of the data by using secure labels

42. The security model defines the data structure and technology required for the security policy. Which of the following best describes the "simple security rules" in the security model?

A. Up up is not allowed in the Biba model

B. Reading down is not allowed in the Biba model

C. Down down is not allowed in the Bell-LaPadula model

D. Up-reading is not allowed in the Bell-LaPadula model

43. To prevent authorized users from making unauthorized modifications to the data, the protection of the data integrity is required, and which of the following items best describes the star or (* -) integrity principle?

A. Down down is not allowed in the Bell-LaPadula model

B. Up-reading is not allowed in the Bell-LaPadula model

C. Up up is not allowed in the Biba model

D. Reading down is not allowed in the Biba model

44. Users of a company's business department need to access business data, who cannot directly access business data, and can only operate business data through external programs. This situation is a part of the following security model?

A. Bell-LaPadula model

B. Biba model

C. information flow model

D. Clark-Wilson model

45. As an information security professional, you are designing access control strategies for information resources for a company. Due to the high personnel mobility of the company, you are prepared to determine the access to information resources based on the group that the user belongs to and their responsibilities in the company. Which of the following access control models should be adopted most?

A. Autonomous Access Control (DAC)

B. Forced Access Control (MAC)

C. Role-Based Access Control (RBAC)

D. Minimum privilege (Least Privilege)

46. Which of the following access control models controls the interaction between subject and object through the access control matrix?

A. Forced Access Control (MAC)

B. Centralized Access Control (Decentralized Access Control)

C. Distributed Access Control (Distributed Access Control)

D. Autonomous Access Control (DAC)

47. Which of the following types of IDS can monitor behavioral characteristics in network traffic and create new databases?

    A. Features-based IDS

    B. The IDS based on neural networks

    C. Statistics are based on the IDS

    D. Host-based IDS

48. Which of the following logical processes should the access control model follow?

    A. Identification, authorization, and certification

    B. Authorization, Identification, and Certification

    C. Identification, certification, and authorization

    D. Certification, Identification, Authorization

49. Which of the following FRR rates is the most accurate in the definition of the error rejection rate (F R R) and FAR) in biometric technology?

    A. FAR belongs to Type I error and FRR belongs to Type II error

    B. FAR is the rate at which an authorized user is wrongly rejected and FRR is a Type I error

    C. FRR belongs to the type I error, and FAR is the number of times the impersonator is rejected

    D. The FRR is the rate at which an authorized user is wrongly rejected, and the FAR belongs to a Type II error

50. When evaluating a biometric system, a unit puts forward very high safety requirements. Accordingly, which of the following technical indicators is the most important to the unit?

    A. Error reception rate (FAR)

    B. Average error rate (EER)

    C. Error rejection rate (FRR)

    D. Error Identification Rate (FIR)

51. Which of the following methods can best meet the two-factor certification requirements?

    A. Smart card and user PIN
    B. User ID and password
    C. Iris scan and fingerprint scanning
    D. Magnetic card and user PIN

52. In the Kerberos structure, which of the following causes a single point of failure?

    A. E-Mail Server
    B. Customer workstation
    C. application server
    D. Key Distribution Center (KDC)

53. In which of the following access control technologies, the database is based on data sensitivity to determine who can access the data?

    A. Role-based access control
    B. Content-based access control
    C. Context-based access control
    D. discretionary access control

54. When a database administrator checks the database for poor performance, he is prepared to improve the database performance by removing normalization (denormanization) operations on some data tables, and which of the following risks will increase?

    A. Inconsistencies in access
    B. deadlock
    C. Unauthorized access to the data
    D. Impairment of the data integrity

55. Which of the following is not a preventative physical control?

    A. security guard
    B. police dog
    C. Access registration form

D. crawl

56. For Information security features, the following statement correct ().

A. The Information security is a system of security
B. The Information security is a dynamic security one
C. The Information security is a borderless security
D. The Information security is an unconventional security

57. Objects of the Information security include having a ().

A. target
B. rule
C. organization
D. personnel

58. To implement Information security, ensure that () reflects business objectives.

A. safe strategy
B. target
C. activity
D. Safety execution

59. To implement Information security requires a path to a (ABCD) Information security consistent with organizational culture.

A. put into effect
B. maintenance
C. supervised
D. improve

60. Key success factors in implementing Information security include ().

A. Effectively promote safety awareness to all managers and employees
B. Distribute Information security policies, guidelines, and standards to all managers, employees, and other partners
C. Provide financial support for Information security management activities

D. Provide appropriate training and education

61. The National security components include the ().

A. Information security

B. Political security

C. economic security

D. Cultural security

62. The following () s belong to assets.

A. information

B. information carrier

C. personnel

D. The Image and reputation of the company

63. Characteristics of the Security threats include the ().

A. uncertainty

B. deterministic

C. objectivity

D. subjectivity

64. The Manage risk's method, specifically including the ().

A. administrative means

B. technical method

C. office procedure

D. legal methodology

65. The basic concepts of the Manage risk include the ().

A. property

B. vulnerability

C. Security threats

D. control measures

66. The contents of the PDCA loop include the ().

A. plan

B. put into effect

C. check up

D. move about

67. In the Information security implementation rules, the specific contents of the security guidelines include the ().

A. Assignment of responsibility

B. Agreed to the Information, the scope of the security management

C. Explain specific principles, standards, and compliance requirements

D. Explain the process of reporting suspicious security incidents

68. In the Information security implementation rules, the specific work of the Information security internal organization includes ().

A. Information security's Management commitment to a..

B. Information security coordination

C. Information security Allocation of Information security Responsibilities

D. Authorization process of the information processing equipment

69. The Information security event classification includes the ().

A. General events

B. Bigger events

C. important event

D. Special major events

70. The Information security disaster recovery construction process includes the ().

A. Goals and needs

B. Strategy and scheme

C. Exercise and evaluation

D. Maintenance, review, and update

71. Important technical management elements in the Information security management process include ().

    A. Disaster recovery plan
    B. Operation and maintenance management capability
    C. Technical support capability
    D. Standby network system

72. The factors to Site safety consider are ()

    A. Site site selection
    B. Site fire prevention
    C. The site is waterproof and moisture-proof
    D. Site temperature control
    E. Site power supply

73. 64 The Automatic fire alarm deployment should be noted for the ()

    A. Avoid areas or equipment that may cause electromagnetic interference
    B. With uninterrupted special fire protection power supply
    C. Leave backup power supply
    D. There are two automatic and child-motion trigger devices

74. The measure that can be taken to reduce Lightning loss is ()

    A. The equipotential connection network shall be provided in the machine room
    B. arrange UPS
    C. Set up the safety protection ground and the shielding ground
    D. According to the electromagnetic pulse intensity of lightning strike in different regions, different regional interfaces are equipotential connected
    E. signal processing circuit

75. Will cause the Electromagnetic leakage to have a ()

    A. indicator
    B. Switch circuit and grounding system
    C. Power cord for the computer system

D. Telephone lines in the machine room

E. signal processing circuit

76. The targets of the Computer information system security include the ()

A. Information confidentiality

B. totality of information

C. service availability

D. Rectibility

77. The goal of Computer information system security protection is to protect the () of the computer information system

A. Physical security

B. security of operation

C. Information security

D. Personnel safety

78. The Computer information system security includes the ()

A. System risk management

B. audit trail

C. backup and recovery

D. Electromagnetic information leakage

79. Computer information system security protection measures include ()

A. safety regulation

B. security administration

C. organizational building

D. institutional improvement

Project 4 Emergency response

80. The Computer information system security management includes the ()

A. organizational building

B. Check in advance

C. institutional improvement

D. Personnel consciousness

81. The nature of the Public information network security supervision work, the ()

A. It is an important part of the public security work

B. It is an important means to prevent all kinds of hazards

C. Is an important means of administrative management

D. It is an important means of fighting against crime

82. General principles of Public information network security supervision work ()

A. The principle of combining prevention and strike

B. The principle of combining the supervision of specialized organs with social forces

C. The principle of combining correction with sanctions

D. The principle of combining education and punishment

83. Information security officer conditions: ()

A. Have a certain professional and technical knowledge of computer network

B. After the computer security officer training, and passed the examination

C. Major capital degree or above

D. No illegal or criminal record

84. What security guarantees should the OS provide, the ()

A. Validation (Authentication)

B. Authorization (Authorization)

C. Data Confidentiality (DataConfidentiality)

D. Data consistency (DataIntegrity)

85. What are the security features of Windows OS's Domain control mechanism, ()

A. User authentication

B. access control

C. audit (Log)

D. Encryption of the data communications

86. From the system as a whole, what aspects does Security vulnerabilities include: ()

A. Technical factors

B. human factor

C. Planning, policy, and execution processes

87. From the system as a whole, the following problems belong to the system Security vulnerabilities()

A. The product lacks security features

B. Products have Bugs

C. Lack of sufficient safety knowledge

D. mistake

88. What is the basic way to deal with the operating system Security vulnerabilities? ()

A. Make the necessary adjustments to the default installation

B. Set strict passwords for all users

C. Install the latest security patches promptly

D. Replace it to another operating system

89. Cause of the OS Security vulnerabilities, ()

A. Unsecure programming language

B. Unsafe programming habits

C. Unwell-considered architectural design

90. What elements of () should a strict Password policy contain

A. Meet a certain length, such as more than 4 or more

B. Contains both numbers, letters, and special characters

C. The system requires periodic password changes

D. Users can set an empty password

91. The Computer security cases includes the following aspects of the ()

A. Application of important safety technologies

B. Implementation of safety standards

C. Construction and implementation of safety system and measures

D. Major hidden safety risks, the discovery of violations of laws and regulations, the occurrence of accidents

92. Computer security cases includes the following content ()

A. Violation of the laws of the State

B. Violation of State regulations

C. Events that endanger or endanger the security of the computer information system

D. Common mechanical failure in computer hardware

93. Major Computer security accident can be accepted by the _____ for ()

A. The public information network security supervision department of the public security organs of the prefecture-level public security organs

B. Public security department of the local county-level (district, city) public security organ where the crime was committed

C. The public information network security supervision department of the local county-level (district, city) public security organs where the crime was committed

D. The local police station where the crime

94. Site investigation mainly includes the following links, _____()

A. Description of the hardware and software of the damaged computer information system and the degree of damage

B. Replication and repair of existing electronic data on site

C. Discovery and extraction of electronic traces, fixation and preservation of evidence

D. Collect and seize articles related to an accident or a case on site

95. Computer security accident Identification of Cause and Data Identification in Computer Case, ____()

   A. Is is a professional technical work
   B. Relevant verification or investigation experiments can be carried out if necessary
   C. Can hire the expert of concerned respect, form expert appraisal group to undertake analysis and appraisal
   D. An appraisal report may be issued by a computer case

96. By choosing one of the safest operating system, the whole system can be safe.（）

   A. exactness
   B. wrong

97. The Password of Screen saver is case.（）

   A. exactness
   B. wrong

98. The basic rule of Password learning is that you have to let the Password analyst know about the methods used for Encryption and decryption.（）

   A. exactness
   B. wrong

99. Social engineering, posing as a legitimate user to send email or call managers to defraud users of password and other information; spam search: Attacker gets information related to the system by searching for the attacked waste. If the user writes the password on paper and throws it casually, it can easily become the Attack object of spam search.（）

   A. exactness
   B. wrong

100. Security management involves physical security, access control, information Encryption, and Network security management policies.（）

   A. exactness
   B. wrong

StageII:Safe operation

Background: As information security technicians must be able to master the operating system reinforcement and security control, firewall general configuration, common service configuration and other related skills, using these skills we can further ensure the smooth operation of important business.

The security operation stage topics mainly include: operating system security reinforcement, iptables firewall configuration, application service security configuration and other contents.

Project 1 System security control

Task 1 Windows reinforcement

As a security operation personnel of Company A, you currently have a Windows system computer that needs to be strengthened. Please complete the relevant operations according to the following requirements to ensure the safe operation of the system.

1. The current system service brief information is listed through the wmic tool, and stores the commands used for the html format are;

2. List the current system user details through the wmic tool, using the command of;

3. With the sc tool management services, the command to start the mysql service is;

4. Managing the Windows Firewall via the command-line CMD, the commands that can connect all ports to 192.168.10.1.100 are;

5. Conuring Windows Firewall through the command line CMD, the command to block tcp / 3389 port connections is;

6. Managing Windows users through the command-line CMD, the command to add skill users to the administrators group is.

Task 2 Linux reinforce

As a security operator of Company A, you currently have a Linux system computer that needs to be strengthened. Please follow the following requirements to ensure the safe operation of the system.

1. The path to store the real-time memory information files in the Linux operating system is;
2. The file path for storing the boot-on automatically mounted disk information in the Linux operating system is;
3. The Linux operating system SSH service disables the root user login The configuration to modify is;
4. The configuration of the Linux operating system SSH service is;
5. The default anonymous user name for the Linux operating system VSFTPD service is;
6. The Linux operating System VSFTPD service disables anonymity and the configuration required is.

Project 2 Firewall security control

Task 3 Workstation firewall configuration

As a security operation personnel of Company A, you currently have a Linux system workstation firewall that needs to be configured. Please complete the relevant operations according to the following requirements to ensure the safe operation of the system.

1. Use iptables firewall to control traffic forwarding, which chain needs to operate;
2. Use the iptables firewall to control traffic access, the option to limit the access traffic IP address is;
3. Use the iptables Firewall to control the default rules to deny all traffic access is;

4. Use the iptables firewall to configure the workstation type firewall, the exit direction will generally perform what operation;

5. Use iptables Firewall to configure the new connection speed of tcp / 22. What is the command required;

6. Which table is required to configure the nat address transformation using the iptables fencing wall;

7. Using the iptables firewall configuration to release the commands from 192.168.1.100 to 192.168.3.100 to use is;

8. When using the iptables firewall to configure the workstation type firewall, which interface traffic should be fully released;

9. When you use iptables Firewall to configure a workstation type firewall, what commands you execute can clear all rules.

Project 3 Application service security

Task 4 The VSFTPD service configuration

As a security operation personnel of Company A, you currently have a Linux system VSFTPD service that needs to be configured. Please complete the relevant operations according to the following requirements to ensure the safe operation of the system.

1. Configuration The configuration for enabling VSFTPD virtual users is;

2. Configure the enabled VSFTPD virtual user file, user name admin password admin user file;

3. Configure modify VSFTPD service port to 2200, firewalld firewall is;

4. Configure the modified VSFTPD service port to 2200, the selinux required action is;

5. Configure fying the VSFTPD service public folder to / srv / ftp / share, selinux is;

6. The command to crack the vsftpd service password by using the hdyra tool (username: admin password dictionary: password.txt) yes;
7. The command to crack the vsftpd service password by using the medusa tool (user name: admin password dictionary: password.txt) yes;

Task 5 The File Sharing Service Configuration

As a security operator of Company A, you currently have a Linux system file sharing service that needs to be configured. Please follow the following requirements to complete the relevant operations to ensure the safe operation of the file sharing system.

1. The command for the Linux operating system to use the yum package manager to install the file sharing service is;
2. The Linux operating system profile sharing directory is in / srv, / samba, and selinux. The required configuration is;
3. The command for the Linux operating System Profile Sharing Service user is;
4. The Linux OS Profile Sharing Service User, the command to create a new user, share, is;
5. The Linux operating system Profile Sharing Service anonymous user access configuration is;
6. Linux operating system profile file Sharing Service share printer, the default share name is;
7. The smbclient tool to view the command for which shared directory usage exists under server 192.168.1.100 is.

Task 6 The Certificate Management Service configuration

As a security operation personnel of Company A, you currently have a Linux system certificate management service that needs to be configured. Please follow the following requirements to complete the relevant operations to ensure the safe operation of the certificate distribution system.

1. Use the cfssl tool to view the default request configuration information and the command used is
2. The command used to initialize the CA certificate by using the cfssl tool is;
3. The command used to initialize the server certificate by using the cfssl tool is;
4. Use the cfssl tool to revoke the test certificate use command is;
5. The command to generate the rsa key is;
6. The command to use the openssl tool to view the certificate information is;

StageIII： Emergency response

Background: As an information security technician, we must be able to master content mirror analysis, important data recovery, malicious file analysis and other related skills. Using these skills, we can immediately analyze relevant malicious files and analyze clues to help us better complete the emergency response work.

The emergency response stage topics mainly include: Window s memory mirror analysis, Linux memory mirror analysis, disk file recovery, malicious program analysis and other content.

Project 1 Memory mirror analysis

Task 1 Windows memory mirror analysis

As an emergency responder of Company A, please analyze the memory files provided to find the relevant key information according to the following requirements, and complete the emergency response event.

1. Get the password of the user admin from the memory and crack the password, and submit it in Flag {admin, password} (the password is 6-bit);

2. Get the current system ip address and hostname, submit in Flag {ip: hostname};

3. Get the keywords searched by the current system browser and submit them as Flag;

4. The mining process exists in the current system, please get the mine pool address that you have pointed to, and submit it as a Flag {ip: port};

5. The malicious process has registered a service in the system, please submit the service name as a Flag {service name}.

Project 2 Confidential data recovery

Task 2 Financial data recovery

As an emergency responder of Company A, please analyze the provided disk files to find the relevant key information and complete the emergency response event.

1. Analyze the file system in the disk mirror to find key financial evidence one
2. Analyze the file system in the disk mirror to find key financial evidence two
3. Analyze the file system in the disk mirror to find key financial evidence three
4. Analyze the file system in the disk mirror to find key financial evidence four
5. Analyze the file system in the disk mirror to find key financial evidence five
6. Analyze the file system in the disk mirror to find key financial evidence six
7. Analyze the file system in the disk mirror to find key financial evidence five
8. Analyze the file system in the disk mirror to find key financial evidence six

Task 3 Express delivery waybill information recovery

As an emergency response officer of Company A, please analyze the provided traffic package file to find the relevant key information according to the following requirements, and complete the emergency response event.

1. Analyze the provided traffic package and find the relevant data of the system waybill information
2. Analyze the provided traffic package, and find the data related to the system waybill information 2
3. Analyze the provided traffic package and find the data related to the system waybill information
4. Analyze the traffic package and find the system waybill information
5. Analyze the found password library of the waybill system administrator, and try to crack the password 1

6. Analyze the password library of the waybill system administrator found, and try to crack the password 2

7. Analyze the found waybill system management data, and find the key waybill record 1

8. Analyze the found waybill system management data, and find the key waybill record 2

Task 4 Encryption system crack

As an emergency response officer of Company A, please analyze the incomplete footsteps documents provided to find the relevant key information according to the following requirements, and complete the emergency response event.

1. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking of the server scenario SSH service login password, fill in the vacant F1 string in the file, and submit the hexadecimal result as the Flag value (form: hexadecimal string);

2. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking of the server scenario SSH service login password, fill in the vacant F2 string in the file, and submit the hexadecimal result as the Flag value (form: hexadecimal string);

3. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking of the server scenario SSH service login password, fill in the vacant F3 string in the file, and submit the string back to the hash decimal result as the Flag value (form: hexadecimal string);

4. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking of the server scenario SSH service login password, fill in the vacant F4 string in the file, and submit the hexadecimal result as the Flag value (form: hexadecimal string);

5. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function

of violent cracking of the server scene SSH service login password, fill in the vacant F5 string in the file, and submit the hexadecimal result as the Flag value (form: hexadecimal string);

6. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking the server scene SSH service login password, fill in the vacant F6 string in the file, and submit the string back to the hash hexadecimal result as the Flag value (form: hexadecimal string);

7. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking the server scenario SSH service login password, fill in the vacant F7 string in the file, and submit the decimal result of the hash value after the SHA256 operation as the Flag value (form: hexadecimal string);

8. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking of the server scenario SSH service login password, fill in the vacant F8 string in the file, and submit the hash result as the Flag value (form: hexadecimal string);

9. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file enables the program to realize the function of violent cracking of the server scenario SSH service login password, fill in the vacant F9 string in the file, and submit the the decimal result of the string after SHA256 operation as the Flag value (form: hexadecimal string);

10. Edit the Python program ssh_brute_force. The py file, utilizing the superdic. The txt password dictionary file makes the program realize the violent crack server scenario SSH service login password function, run the program, run the correct password after the program returns the hash hex result as the Flag value (form: hexadecimal string) submitted;

Project 3 The APT attacks are traceable

Task 5 Attack flow traceability

As an emergency response officer of Company A, an important department in the company operates an APT attack. Now, if you capture the relevant traffic, please find the key information according to the following requirements and complete the emergency response event.

1. Use Wireshark to view and analyze the login under the server scenario desktop.pcapng packet file, by analyzing the package login. In the pcapng message No.130, identify the valid command submitted by the hacker, and submit the valid command as a FLAG (form: [command]);

2. Continue viewing the package file login.pacapng, analyzes what command the hacker has executed, and submits the valid command as a FLAG (form: [command]);

3. Continue viewing the package file login. After pacapng analyzes that the hacker performs the above command, the multiple IP addresses in the resulting results are submitted as FLAG (form: [IP address 1: IP address 2: IP address n]);

4. Continue viewing the package file login.pacapng analyzes that after the hacker performs the above command, the last 1 physical address in the resulting result is submitted as FLAG (form: [physical address]);

5. Continue viewing the package file login.pacapng analyzes the valid command used by the hacker to establish the mapping, and submits the IP address in the command as a FLAG (form: [IP address]);

6. Continue viewing the package file login.pacapng analyzes the valid command used by the hacker to establish the mapping, and submits the user name in the command as an FLAG (form: [user name]);

7. Continue viewing the package file login.pacapng analyzes the valid command used by the hacker to establish the mapping, and submits the password in the command as a FLAG (form: [password]);

Task 6　Server log analysis

As an emergency response officer of Company A, an important server in the company is attacked. When the traffic package is captured, please obtain the key information as required below and complete the emergency response event.

1. Use Wireshark to view and analyze the logs under the server scenario desktop.pcapng packet files, by analyzing the package logs. The pcapng finds out the ninth file scanned by the malicious user directory, and uses the file name as the FLAG (form: [robots.txt]) submit to;

2. Continue viewing the package file logs.pcapng, analyzes which ports are scanned by malicious users, and submit all ports as FLAG (form: [port name 1, port name 2, port name 3..., port name n]) from low to high;

3. Continue viewing the package file logs. The pcapng has figured out what the malicious user reads the server's file name is, and uses it as a FLAG (form: [robots.txt]) submit to;

4. Continue viewing the package file logs.pcapng analyzes what the path that the malicious user writes to a sentence Trojan is, and submits the path as a FLAG (form: [/ root / whoami /]);

5. Continue viewing the package file logs.pcapng analyzes what is the password for the malicious user to connect to a one-sentence Trojan horse, and submits the one-sentence password as a FLAG (form: [one-sentence password]);

6. Continue viewing the package file logs. The pcapng analyzes what files the malicious user has downloaded, and uses the file name and suffix as the FLAG (form: [File name). Suffix name]) Submit;

7. Continue to view the packet file logs.pcapng submits the content of the files downloaded by malicious users as FLAG (form: [file content]);

StageIV： CTF capture the flag

Background: As an information security technician, in addition to mastering the safe operation, emergency response and other aspects of safety content, he should also often participate in the CTF flag winning actual combat. Through the flag winning competition, he can further improve the actual combat technical ability, hone the patience of players, and enhance the learning ability of players.

The title of CTF flag capture stage mainly includes: injection attack, template escape, serialization vulnerability, service vulnerability and other related content.

Project 1 Injection attack

Task 1 Command injection

1. Open the Firefox browser on the permeating machine, enter the IP address of the target machine server in the address bar to access the web page, log in with the default user name admin password password, click the "DVWA Security" button in the left navigation bar on the DVWA page, modify the difficulty to "low", and then click "Submit" to submit. Click "Command Injection" to enter the target machine server IP, and you can see the normal return data, and submit the first word of the last row of the returned data as the Flag value.

2. A construction statement displays the user in the operating system, submitting parts of the construction statement other than the IP address as a Flag value.

3. Click "DVWA Security" on the DVWA page to select the difficulty degree of "medium", then click "Submit" to submit, and again use the above construction statement to display the user in the system, find that the error is reported, and submit the penultimate second word of the returned result as the Flag value.

4. Click "view_source" to view the source code, submitting the filtered content in the source code as F1.F2 as a Flag value.

5. Reconstruction statements that display users in the operating system, see the normal return data, and commit parts of the reconstruction statement other than the IP address as a Flag value.

6. Click "DVWA Security" on the "DVWA page" to select the difficulty of "high", and then click "Submit" to submit, resubmit the reconstructed statements in the previous step, find the error report, click "view_source" to view the source code, and found that the server has further filtered the IP parameters, submitting the third filtered content in the source code as the Flag value.

7. Reconstruct statement is used to display the users in the operating system, you can see the normal return data, and commit the part of the reconstruct statement other than the IP address as the Flag value.

8. Again, the construction statement is used to display the users in the operating system, and you can see the normal return data, submitting the last user name in the returned user list as the Flag value.

Task 2 SQL pour into

1. The system has a vulnerability, log in to the system to find the hidden information, and submit the flag;

2. The system has a vulnerability, to find the database user name used by the current WEB system;

3. The system has a vulnerability in finding the hidden information in the database and submitting the flag.

Project 2 Serial vulnerability

Task 3 Serialized strand utilization

1. Access the target machine address, and submit the PHP _ SHA256 value in the target machine P H P environment as the flag;

2. Accessing the target machine address and taking the top 6 digits of the variable content sent through the GET method as the flag submission;

3. Access the target machine address, and make the name of the special HTTP header variable required to complete the topic configuration as a flag submission;

4. Access the target machine address and submit the function name required to bypass the completion topic as a flag;

5. Access the target machine address, and submit the request method required to complete the topic as a flag;

6. Access the target machine address and use the deserialization vulnerability in the topic to submit the flag in the target machine environment.

Task 4 Serialized string escape

1. Access Target port 8081 and will view index via pseudo protocol. The payload of the php file is submitted as a flag;

2. Take the result obtained from issuing the serialized string escape as a flag submission;

3. Complete the POP chain deserialization and submit the resulting file name as a flag;

4. Crack the file found in the previous title, and submit the found file name as a flag;

5. Crack the file found in the previous title, find the file name as a flag and submit it;

6. Use the information found to log in the system to complete the rights, obtain the final flag and submit.

Project 3 Service vulnerability

Task 5 File upload

Access the target machine address port 9000 and submit the function name of the user display code in the page as a flag;

Submit the type of session in the program as a flag;

Raise the PHPSSID required to get admin user permission as a flag price;

Submit the first four file names required to be uploaded to complete the title as a flag;

Submit the session file save location in the title environment as a flag;

The last 9 bits of the session file to be downloaded to are the most flag submitted;

Will / app / session / success. The Type of txt is submitted as a flag;

Complete the title and submit the last obtained flag value as a flag.

Task 6 Buffer overflow vulnerability

1. Download the flag0001.exe from the FTP of the target machine server, analyze the file, and please submit the encryption function used by the program;
2. Please submit the Key value that the program runs properly for use;
3. Please submit the overflow point address;
4. Please submit the secret key for the encryption algorithm;
5. Please submit the value of the final flag.