The First World Vocational College Skills Competition

Innovations in Information Technology Applications

Test Projects

Instructions for the Competition

I. Release of the Competition Content

The "Network Building and Application" competition contains three parts, including:

Part 1: IT Innovation Service Operation and Maintenance (600 Points), Competition Duration: 240 Minutes.

Part 2: IT Innovation CTF (200 Points), Competition Duration: 120 Minutes.

Part 3: IT Innovation Security Confrontations (200 Points), Competition Duration: 60 Minutes.

II. Competition Precautions

1. It is forbidden to carry and use mobile storage equipment, calculators, communication tools and reference materials.

2. Please check whether hardware equipment the lists of software list and materials are complete in line with the competition environment provided by the Competition and whether computers are normal.

3. Competitors should carefully read the competition paper and complete all operations in accordance with the requirements in the competition paper.

4. Equipment configurations should be timely saved during operation.

5. All equipment should remain operating at the end of the Competition. Judgment should be subject to the final hardware connection and configurations.

6. Upon the completion of the Competition, competition equipment, software and Test Projects should be kept at the workstation. It is forbidden to take all competition supplies (including the competition paper and scratch paper) away from the workshop.

7. It is forbidden to make any marks not related to the Competition on paper materials and competition equipment. In case of rule violations, zero marks would be granted.

8. Tool software related to the Competition should be kept in D:\soft in each host.

Project profile:

After the outbreak of the pandemic in 2021, the company has planned to continue a strategic plan decided previously. Under the leadership of the group's senior executive. the company's size has resumed rapid growth in the second half of the year, followed by significant increases in the volume of business data and company visits. In order to better manage data and provide services, the group has decided to add two IT innovation servers and PCs to the two Internet Data Centers (IDCs) and deploy some applications for testing.

Topology:

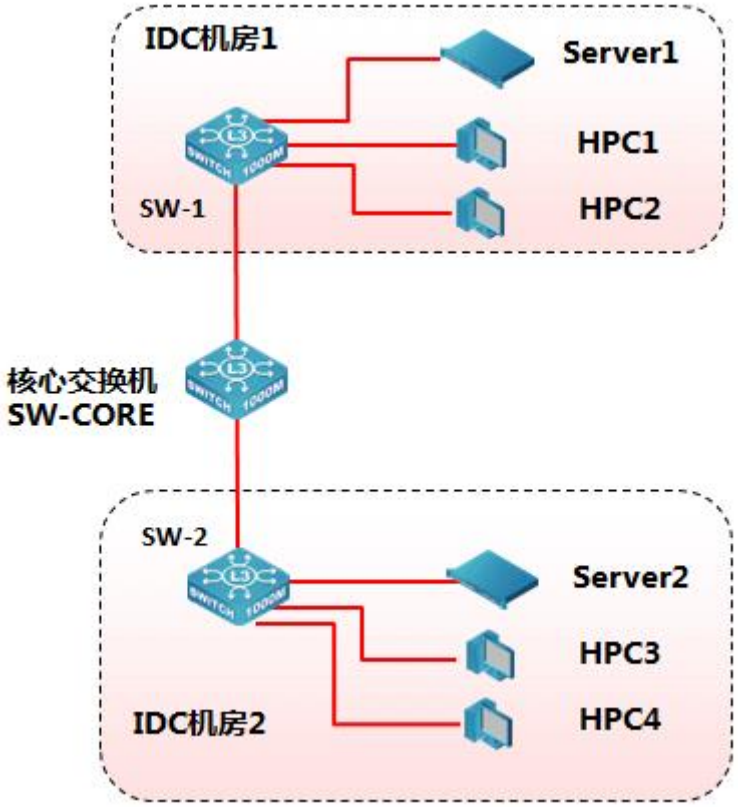

Table of Network Equipment Connection:

Equipment A is connected to Equipment B			
Equipment name	**Interface**	**Equipment name**	**Interface**
SW-1			
SW-2			
SW-CORE			
Server1			
Server2			
HPC1			
HPC2			
HPC3			
HPC4			

Name of virtual machine	Domain name	Service role	Information of IPv4
Server1			
Linux-1	cs1.skills.com	Domain Name Server (DNS) service Certification Authority (CA) service Chrony service	10.10.70.11
Linux-2	cs2.skills.com	Domain Name Server (DNS) service Mail service Docker service	10.10.70.12
Linux-3	cs3.skills.com	Apache2 service MariaDB service Hypertext Preprocessor (PHP) service Rsyslog service	10.10.70.13
Linux-4	cs4.skills.com	MariaDB client Rsyslog client	10.10.70.14
Server2			
Linux-5	cs5.skills.com	Internet Small Computer System Interface (iSCSI) service	10.10.70.15 10.10.80.16
Linux-6	cs6.skills.com	Keepalive cluster	10.10.70.16 10.10.80.17
Linux-7	cs7.skills.com	Keepalive cluster	10.10.70.17 10.10.80.18

Operation and Maintenance of the IT Innovation Network (600 points)

Competition Duration: 240 Minutes

I. Building and Launch of the IT Innovation Server (50 Points)

Elevation of the right routing panel

Elevation of the left routing panel

[Instructions]

1. The left routing panel of the cabinet is numbered 101; the right routing panel of the cabinet is numbered 102.
2. When you face the information bottom cases, Port 1 will be on the left and Port 2 will be on the right. All distribution frames and modules are terminated in line with the connection method for 568B standard ports.
3. See the following table for the correspondence of wiring points between the main distributing district and the working area.
4. Table of the Correspondence of Wiring Points Between PC1 and PC2

No.	Information point No.	Distribution frame No.	Bottom case No.	Information point No.	Port No. of distribution frame
1	W1-02-101-1	W1	101	1	02
2	W1-06-102-1	W1	102	1	06

I. Laying and Termination of Cables

1. Take two twisted pairs in an appropriate length, label the two ends, and pass them

through PVC wiring ducts or tubes. Reasonably wire the twisted pairs inside the cabinet and fixate them with cable ties.

2. Terminate one end of the two twisted pairs to the corresponding port of the distribution frame in line with "Table of the Correspondence of Wiring Points Between PC1 and PC2".
3. Terminate the other end of the two twisted pairs to the RJ45 module in line with "Table of the Correspondence of Wiring Points Between PC1 and PC2", install the information point panel, and label them.

II. Production and Testing of Jumper Wires

1. Take another two twisted pairs in an appropriate length and label the two ends. Connect network information points and the corresponding computers, and terminate crystal heads to produce network jumper wires in line with "Table of the Correspondence of Wiring Points Between PC1 and PC2". Produce all network jumper wires in accordance with 568B standards.
2. In accordance with network topology requirements, take twisted pairs in an appropriate length and number and terminate crystal heads to produce network jumper wires. In line with the requirements of Test Projects, insert the network jumper wires to the relevant ports of the corresponding equipment (including between equipment and between equipment and distribution frames).
3. Interconnect PCs, the information point panel, distribution frames and equipment. (Tip: The equipment coming with the cabinet can be used to test connection and disconnection.)

PC1 is connected to Port 1 of Bottom Case 102; PC2 is connected to Port 1 of Bottom Case 101.

III. Launch of the IT Innovation Server

1. Launch the IT innovation server in line with comprehensive routing standards.
2. Use twisted pairs or optical fiber cables to connect the IT innovation server for High Performance Computing (HPC) to a switch.

II. Building of the IT innovation Network (100 Points)

1. In order to reduce broadcasting, VLAN should be planned and configured, according to the requirements of Test Projects. Configures should be reasonable. It is forbidden for unnecessary VLAN data flows, including VLAN 1, to pass all links. VLAN configurations and port distribution should be completed on the switch in accordance with the following information and table.

Device	VLAN No.	Port	Notes
SW-1	VLAN10	E1/0/1-4	Marketing Segment 1
	VLAN20	E1/0/5-7	Product Segment 1
	VLAN30	E1/0/8-10	Legal Segment 1
	VLAN40	E1/0/11-12	Financial Segment 1
	VLAN50	E1/0/13-14	HR Segment 1
SW-2	VLAN10	E1/0/1-4	Marketing Segment 2
	VLAN20	E1/0/5-7	Product Segment 2
	VLAN30	E1/0/8-10	Legal Segment 2
	VLAN40	E1/0/11-12	Financial Segment 2
	VLAN50	E1/0/13-14	HR Segment 2
SW-3	VLAN20	E1/0/1-6	Product Segment 3
	VLAN30	E1/0/7-11	Legal Segment 3
	VLAN50	E1/0/12-15	HR Segment 3

2. The Telnet login function of the group's core switches, SW-1 and SW-2, should be enabled. The following information of authorization should be displayed prior to the login to the terminal interface through Telnet, "WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility".

3. For the group's core switches, SW-1, SW-2 and SW-CORE, three bare optical cable channels should be rented from an operator to achieve interconnection between two DCs. One bare optical cable channel should be used to achieve the layer-3 IP business, while one carries the VPN business; and the last one carries

the layer-2 business. Specific requirements are as follows:

4. In order to save the group's costs, the bandwidth of the bare optical cable channel carrying the VPN business is only 10 Mbps. It would be based on business whether the bandwidth should be expanded. Relevant technologies should be used to separate the routing table of the group's Financial Segments 1 and 2 from the routing table of other business segments.
5. Currently, only one bare optical cable channel is used to carry the layer-2 business. As the group's IDC servers increase rapidly, it is expected that the next two to three years will witness an explosive growth of the layer-2 traffic of the group's DC servers. Relevant technologies should be configured for the convenience of the expansion and redundant backup of subsequent links.
6. SW-CORE, as one of the group's core switches, separates the routing table of the group's financial business from that of other businesses. The Internet routing table is inside the VPN instance name, Internet.
7. Relevant functions should be configured to enable the group's core switches, SW-1, SW-2 and SW-CORE, to find each other in the network and share information of their respective systems and configurations. Therefore, the administrator can check the correspondence between two interfaces and judge the communication state of links.

III. Operation and Maintenance of the IT innovation System (400 Points)

1. Domain Name Server (DNS) service

1. Set the time zone of all Linux servers as "Shanghai" and adjust the local time to the actual time.
2. Enable the firewalls of all Linux servers and add the corresponding port (it is not allowed to add services) to release relevant services.
3. Use Chrony to configure Linux-1 so as to provide other Linux hosts with time synchronization services.
4. Use bind9 to configure Linux-1 as the main DNS server and adopt RNDC to provide uninterrupted DNS services. Configure Linux-2 as the standby DNS server to provide all Linux hosts with redundant DNS forward and reverse resolution services.
5. The root users of all Linux hosts use a fully qualified domain name (FQDN) to log in other Linux hosts through SSH access without a password.
6. Configure Linux-1 as a CA server to grant all Linux hosts certificates. It is not allowed to modify /etc/pki/tls/openssl.conf. A CA certificate is valid for 20 years. All certificates granted by CA is valid for 10 years. Certificate information: Country = "CN", province = "Beijing", city = "Beijing", organization = "skills", organizer = "system". No certificate warnings will appear, when https websites are visited through Google Chrome.

2. Mail service

1. Configure Linux-2 as the mailserver and install postfix and dovecot.
2. Only support smtps and pop3s connections. The certificate path is

/etc/ssl/mail.crt, and the private key path is /etc/ssl/mail.key.

3. Create users, mail1 and mail2. An email sent to all@skills.com should be received by each user.
4. The root user uses the mail tool to send an email to all@skills.com, with the email subject "Hello" and the main body of "Welcome".

3. Apache2 service

1. Configure Linux-2 as the httpd server and install apache2. Automatically direct to an https safe link, when an http website is visited.
2. Adopt LDAP to certify users. Only the certified users, user1 and user2, can access websites.
3. Automatically direct to www.skills.com, when skills.com or any.skills.com (any represents any URL prefix) is visited.
4. Close unsafe server information. The version information of the system and the WEB server will not appear on any page.
5. For client access, an SSL certificate is a must.

4. Rsyslog service

Configure Linux-3 as the remote log server to provide log services to Linux-4.

5. MariaDB service

1. Configure Linux-3 as the MariaDB server and install MariaDB-server. Create the database user, jack, who will have complete permissions over all databases on any machine. Remote login by the root user is accepted.
2. Configure Linux-4 as the MariaDB client, design and write a Python program, mariadb2.py, in the directory, /app, and create a database, userdb. Create a table, userinfo, in the database, insert two entries in the table, namely (1, user1,

1995-7-1, male) and (2, user2, 1995-9-1, female). The passwords and the usernames are the same. Encrypt the password field with the password function. See the table structure below:

Field Name	Type of Data	Primary key	Auto-increment
id	int	Yes	Yes
name	varchar(10)	No	No
birthday	datetime	No	No
sex	char(5)	No	No
password	char(200)	No	No

3. Design and write a Python program, mariadb3.py, in the directory, /app, modify the structure of the table, userinfo, add a new field, height (type of data: float), to the name field, and update the field of height of user1 and user2 to 1.61 and 1.62.
4. Export the content of /soft/mysql.txt in the physical server to the table, userinfo, and encrypt the password field with the password function.
5. Export the records in the table, userinfo, and save them in the file, /var/databak/mysql.sql.

6. Hypertext Preprocessor (PHP) service

1. Install PHP on Linux-3 to build a PHP network.

7. keepalive service

1. Add four hard disks to Linux-5, whose size is 5G each, and create Logical Volume Manager (LVM). The name of volume group is vg1, and the name of logical volume is lv1. The capacity is all the space. Format the hard disks as ext4. Use /dev/vg1/lv1 to configure the iSCSI target server and provide Linux-6 and Linux-7 with iSCSI services. The wwn of the iSCSI target is iqn.2021-05.com.skills:server, and that of the iSCSI initiator is iqn.2021-05.com.skills:client.

2. Configure Linux-6 and Linux7 as iSCSI clients.
3. Configure Linux-6 and Linux-7 as cluster servers and install keepalive. Linux-6 is the main server, while Linux-7 is the backup server. The virtual IP address is 10.10.70.90. Provide apache services. The domain name is www2.skills.com. The home page of the website index.html is "HelloLinuxCluster".

8. Virtualization

1. Install Linux-2 on docker-ce and import the CentOS mirror. Save the software package and the mirror in the physical server, /soft/DockerLinux.

Create a container named skills, map Port 80 of Linux-2 to Port 80 of the container, and install apache2 in the container. The default content of the webpage is "HelloContainer".

IV. Professional Quality (50 Points)

IT Innovation CTF (200 points)
Competition Duration: 120 Minutes

There are several IT innovation servers in the group's IDC network, each of which is corresponding to different business services. Certain network security risks exist in the network, please use your mastered penetration testing techniques, and complete the penetration test of the specified project through information collection, vulnerability mining and other penetration testing techniques to obtain the flag value in the test.

The penetration testing techniques used in this module include, but are not limited to, the following technical areas:

- Information collection
- Reverse file analysis
- Binary vulnerability exploitation
- Application service vulnerability exploitation
- Miscellaneous and cryptographic analysis

Task I. The WEB server

1. There is hidden information in the Web server system, please find out the hidden information and submit the flag. flag format flag{<flag value>}

2. The Web server system is vulnerable, please take advantage of the vulnerabilities to find out and submit the flag. flag format flag{<flag value>}

3. The backend of the Web server system is vulnerable, please take advantage of the vulnerabilities to find out and submit the flag. flag format flag{<flag value>}

Task II. The FTP server

1. Please obtain and analyze the corresponding file in the FTP server, and find out

and submit the hidden flag. flag format flag{<flag value>}

2. Please obtain and analyze the corresponding file in the FTP server, and find out and submit the hidden flag. flag format flag{<flag value>}

3. Please obtain and analyze the corresponding file in the FTP server, and find out and submit the hidden flag. flag format flag{<flag value>}

4. Please obtain and analyze the corresponding traffic packet in the FTP server, and find out and submit the hidden flag. flag format flag{<flag value>}

5. Please obtain and analyze the corresponding file in the FTP server, and find out and submit the hidden flag. flag format flag{<flag value>}

6. Please obtain and analyze the corresponding file in the FTP server, and find out and submit the hidden flag. flag format flag{<flag value>}

Task III. The application server

1. Port 10000 of the application server is vulnerable, find out and submit the hidden flag. flag format flag{<flag value>}

2. Port 10001 of the application server is vulnerable, find out and submit the hidden flag. flag format flag{<flag value>}

3. Port 10002 of the application server is vulnerable, find out and submit the hidden flag. flag format flag{<flag value>}

4. Port 10003 of the application server is vulnerable, find out and submit the hidden flag. flag format flag{<flag value>}

5. Port 10004 of the application server is vulnerable, find out and submit the hidden flag. flag format flag{<flag value>}

Task IV. Application of big data and machine learning: Web security testing

Instructions on the task environment:

Attacker:

Physical server:

Virtual Machine 1:

Installation for Virtual Machine 1: Python/Python3/GDB

Virtual Machine 1: Username: root, password: 123456

Operating System 2 of Virtual Machine: CentOS_Linux

Installation for Virtual Machine 2: GDB

Virtual Machine 2: Username: root, password: 123456

Operating System 3 of Virtual Machine:

Installation for Virtual Machine 3: OllyICE

Virtual Machine 3: Username: administrator, password: 123456

Target machine:

Server scenario:

FTP service account of the server scenario: Anonymous

Task details:

1. Download data set files from the FTP server in the server scenario of the target machine: DS01, DS02, and the script of the machine learning algorithm: WebSec.py, and improve the script to implement the following tasks (A, B and C): A. Represent the eigenvectors of data sets to obtain eigenmatrices. B. Use the eigenmatrices to train a model detecting Web security abnormalities. C. Use the model detecting Web security abnormalities to judge whether there are abnormalities in the URL requests in the list. Supplement the vacant character string, FLAG01, in the script, and consider the hexadecimal result of the hash

value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string).

2. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG02, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
3. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG03, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
4. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG04, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
5. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG05, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
6. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG06, in the script, and consider the

hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)

7. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG07, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
8. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG08, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
9. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG09, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)
10. Continue to improve the script, WebSec01.py, in Question 1 of this task, supplement the vacant character string, FLAG10, in the script, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string as the flag value and submit it (form: hexadecimal character string)

11. Execute the program file, WebSec01.py, through the Python interpreter, use the model detecting Web security abnormalities to judge whether there are abnormalities in the URL requests in the list, and consider the hexadecimal result of the hash value, returned through MD5 operation, of the character string returned in the test result, as the flag value and submit it (form: hexadecimal character string).

IT Innovation Group Confrontations (200 Points)
Competition Duration: 60 Minutes

Suppose competitors are the group's information security engineers who take charge of server maintenance. The IT innovation server may have different problems and vulnerabilities (see the list of vulnerabilities below). You should reinforce the server as soon as possible, because many white hat hackers (competitors from other teams) will conduct penetration testing over the sever 15 minutes later.

Tip 1: No need to save documents in this question.

Tip 2: Vulnerabilities in the server can be routine vulnerabilities or system vulnerabilities.

Tip 3: Routine vulnerabilities should be reinforced.

Tip 4: Penetration testing could be conducted over other teams' systems to obtain the flag value and submit it to the judges' server.

Precautions:

Point 1: At no time should Ports 80, 3306 and 5555 of the server be artificially closed, otherwise the team would be ordered to stop the Competition, and granted zero score for Phase III.

Point 2: The judges' server should not be attacked, otherwise the team would be ordered to stop the Competition and granted zero score for Phase III.

Point 3: Any server should not be attacked during the reinforcement phase (the first 15 minutes, subject to on-site judges' instructors), otherwise the attacker would be ordered to stop the Competition and granted zero score for Phase III.

Point 4: The flag value is the unique and only identifier of each protected server. The flag value of the target machine is saved in the file ./root/flaginfoxxxx.xxx.txt. Point 5: A

team should not artificially and maliciously destroy its own server's flag value, otherwise the team would be ordered to stop the Competition and granted zero score for Phase III.

In this process, all competitors can continue to reinforce their own servers and attack other competitors' servers.

List of vulnerabilities:

1. Websites on the target machine may have Command Injection vulnerabilities. Competitors are required to find out Command Injection-related vulnerabilities and take advantage of them to obtain some permissions.

2. Websites on the target machine may have File Upload vulnerabilities. Competitors are required to find out File Upload-related vulnerabilities and take advantage of them to obtain some permissions.

3. Websites on the target machine may have File Include vulnerabilities. Competitors are required to find out File Include-related vulnerabilities and combine them with other vulnerabilities to obtain some permissions and conduct extraction.

4. Services provided by the operating system may have Remote Code Execution (RCE) vulnerabilities. Users are required to find out services with RCE-related vulnerabilities and take advantage of them to obtain system permissions.

5. Services provided by the operating system may have Buffer Overflow vulnerabilities. Users are required to find out services with Buffer Overflow-related vulnerabilities and take advantage of them to obtain system permissions.

6. The operating system may have some System Backdoors. Competitors may find out the backdoors and take advantage of the reserved backdoors to directly obtain system permissions.

Competitors should, through all the above vulnerabilities, obtain the highest permission of the target machines of other competitors, and obtain and submit the flag values of the target machines of other competitors.