Information Security Management and Evaluation Phase I

Network System Integration and Security Protection

（Sample）

Table of Contents

Test Projects for the Competition in Phase I (Sample)

This document contains the Test Projects for the Information Security Management and Evaluation Skill Competition in the First World Vocational College Skills Competition ("Competition") - Phase I, which includes network platform construction, network security equipment configuration and protection.

The duration of the competition is 240 minutes.

Introduction

Competition phase	Task stage	Competition task
Phase I Network system integration and security protection	Task 1	Network system integration
	Task 2	Network system security reinforcement

Required Equipment, Machinery, Devices and Materials

All test items can be completed by the competitors based on the equipment and software specified in the infrastructure list.

Marking Scheme

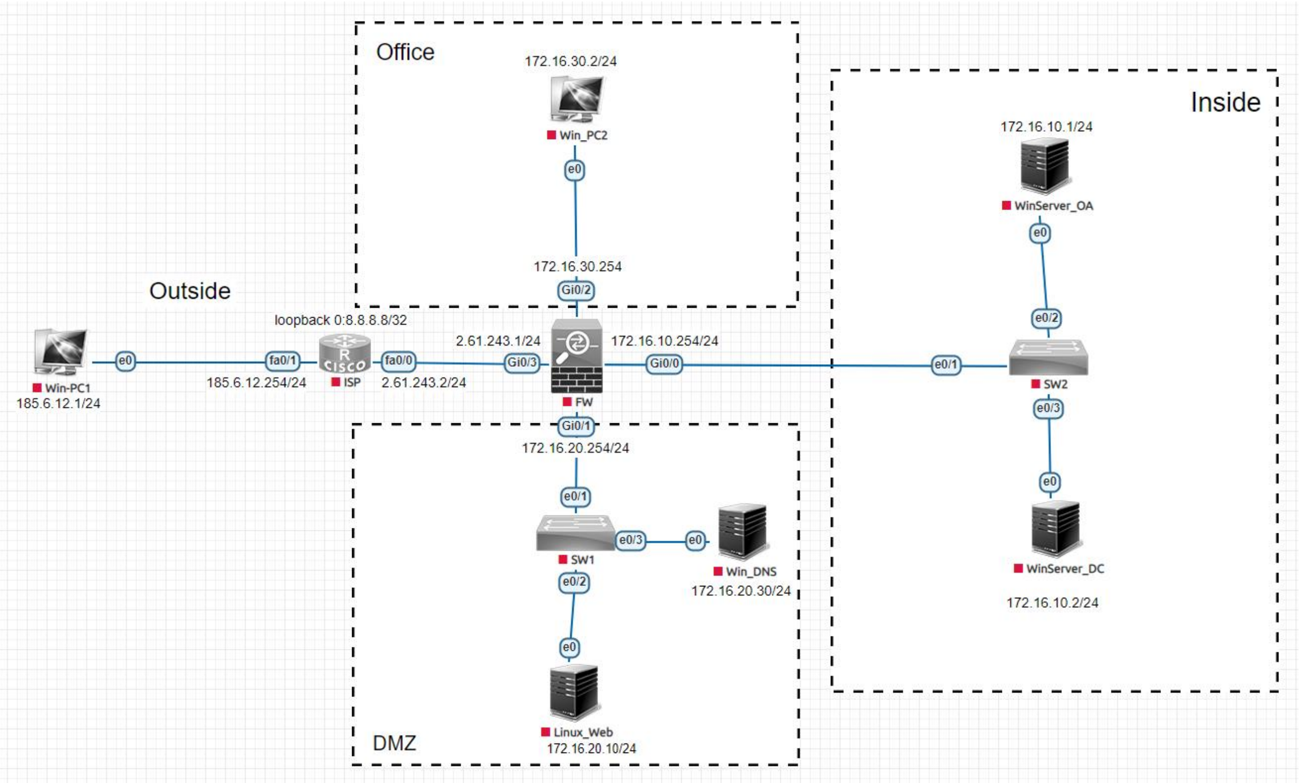
The total score for Phase I is 40 points.

Points for Attention

The marking method of this Competition is computerized testing. Competitors are required not to change their user names and passwords to non-specified passwords in the course of test-taking. If the judge is unable to log into the system and cannot verify the results of the question, the question will not be marked.

Description of Test Projects and Tasks

1. Network topology diagram



2. IP address planning table

Equipment name	Interface	IP address	Notes
ISP	fa0/0	2.61.243.2/24	Connect to Win_PC1
	fa0/1	185.6.12.254/24	Connect to FW Gi0/2
	loopback 0	8.8.8.8/32	Management address
FW	Gi0/0	172.16.10.254/24	Inside area
	Gi0/1	172.16.20.254/24	DMZ area
	Gi0/2	172.16.30.254/24	Office area
	Gi0/3	2.61.243.1/24	Outside area
SW1	e0/1	-	Connect to FW Gi0/1
	e0/2	-	Connect to Linux_web
	e0/3	-	Connect to Win_DNS
SW2	e0/1	-	Connect to FW Gi0/0
	e0/2	-	Connect to WinServer_DC
	e0/3	-	Connect to WinServer_OA

3. Basic server and client configuration

Win_PC1

- Regular user/login password: skills/Worldcolleges2022
- Super admin/login password: administrator/Worldcolleges2022
- Network address/mask/gateway: 185.6.12.1/24/none

Win_PC2

- Regular user/login password: skills/Worldcolleges2022
- Super admin/login password: administrator/Worldcolleges2022
- Network address/mask/gateway: 172.16.30.2/24/172.16.30.254

Linux_Web

- Fully qualified domain name: web.Worldcolleges.com
- Regular user/login password: skills/Worldcolleges2022
- Super admin/login password: root/Worldcolleges2022
- Network address/mask/gateway: 172.16.20.10/24/172.16.20.254

Win_DNS

- Fully qualified domain name: dns.Worldcolleges.com
- Regular user/login password: skills/Worldcolleges2022
- Super admin/login password: administrator/Worldcolleges2022
- Network address/mask/gateway: 172.16.20.30/24/172.16.20.254

WinServer_DC

- Fully qualified domain name: dc.Worldcolleges.com
- Regular user/login password: skills/Worldcolleges2022
- Super admin/login password: administrator/Worldcolleges2022
- Network address/mask/gateway: 172.16.10.1/24/172.16.10.254

WinServer_OA

- Fully qualified domain name: oa.Worldcolleges.com
- Regular user/login password: skills/Worldcolleges2022
- Super admin/login password: administrator/Worldcolleges2022
- Network address/mask/gateway: 172.16.10.2/24/172.16.10.254

Phase I Test Project

Task 1: Network system integration

1. Complete the basic configuration of each network device and operating system based on the topology diagram and network address planning.
2. Please configure the ISP so that PCs in the Outside area can access the DMZ area.

3. Please configure FW to divide Office, DMZ, Inside area as trust area and Outside area as untrust area, so that trust area can access each other and untrust area cannot access trust area.

4. Configure the SNAT function on the DCFW to enable the Office area to access the Outside area.

5. Please configure FW and use 2.61.243.220 for Web IP mapping and allow users in Outside, Inside and Office areas to access Web services.

6. Complete the installation and deployment of domain controller on WinServer_DC, and add WinServer_OA and Win_DNS to domain controller.

7. Complete the installation and deployment of Apache on Linux_Web.

8. Complete the installation and deployment of DNS on Win_DNS.

9. Complete the installation and deployment of IIS Web Server on WinServer_OA.

Task 2: Network system security reinforcement

1. On WinServer_DC, check the Kerberos policy and set the "Service ticket maximum lifetime" value to 342, and apply it to the domain members.

2. On WinServer_DC, check "Configure Kerberos allowed encryption type", set the encryption type to aes256_hmac_sha1, and apply it to the domain members.

3. On WinServer_DC, check the password policy, enable "Password must meet complexity requirements", set the "Mandatory password history" value to 18 and apply it to domain members.

4. On WinServer_DC, check the password policy, set the "Password length minimum" value to 12 and apply it to the domain members.

5. On WinServer_DC, check the password policy and set the value of "Maximum password age" to 26 and apply it to the domain members.

6. On WinServer_DC, check the objects that can access this computer from the network, keep only the administrators group, remove the rest of the unnecessary objects, and apply them to the domain members.

7. On WinServer_DC, enable SYN flood protection for the system, set the threshold for TCP connection requests that have been retransmitted at least once in the SYN_RCVD state to 400, and apply it to domain members.

8. On WinServer_DC, check the "Account lockout threshold", set the threshold to 10, and apply it to the domain members.

9. On Linux_web, check the password policy and convert the configured command for the current password expiration date to an md5 value.

10. On Linux _Web, set the password security policy that will lock the account for five minutes and the root account for ten minutes for three consecutive wrong password entries.

11. On Linux _Web, configure the SSH security policy and change the SSH default port to 5000.

12. On Linux _Web, configure the SSH security policy to allow sshd remote connections only for users on the 172.16.30.0/24 network segment.

13. On Linux_Web, configure Apache security policy to block access to the 172.16.10.0/24 network segment.

14. On Linux_Web, configure the Apache security policy and set the timeout for remote connections to 10.

15. On WinServer_OA, configure and enable CA certificate, and issue customer certificate for Win_PC2.

Marking Distribution Table

Table 1 Marking Table for Phase I

No.	Description	Marking
A	Network system integration and security protection	
A1	Network system integration	
A2	Network system security reinforcement	

Information Security Management and Evaluation Phase II

Response to Network Security Incidents

Digital Forensics and Investigation

Application Security

(Sample)

Test Projects for the Competition in Phase II (Sample)

This document contains the test projects for the Competition - Phase II, which includes response to network security incident, digital forensics and investigation and application security.

The duration of the competition is 180 minutes.

Introduction

The competition has a fixed start and end time, and teams must decide how to allocate their time effectively. Please read the following guidelines carefully!

(1) When the competition is over, please do not turn off your phone when you leave;

(2) All configurations should be valid after reboot;

(3) Do not modify the configuration of the physical machine or the hardware settings of the virtual machine itself except for the CD-ROM/HDD/NET drive.

Required Equipment, Machinery, Devices and Materials

All test projects can be completed by the competitors based on the equipment and software specified in the infrastructure list.

Marking Scheme

The marks for this project module is 30 points.

Description of Test Projects and Tasks

As the network and information technology continues to develop, cybersecurity incidents have proliferated, and various cyber attacks such as network malicious code dissemination, information theft, information tampering, and remote control have seriously jeopardized the confidentiality, integrity, and availability of information systems. Therefore, counteracting cyber attacks, organizing emergency response to security incidents, collecting electronic evidence and other technical work are an essential component of network security protection. Now, Group A has suffered an illegal malicious attack from an unknown organization, your team needs to help Group A trace the source of this cyber attack, analyze the evidence trail of the malicious attack, identify the vulnerability or malicious code in the operating system and application, and help them strengthen their network security defense.

This module is mainly divided into the following sections:

- Response to network security incident
- Digital forensics and investigation
- Application security

All task materials or environments in this section have been placed on the designated computer, and competitors will fill in the "Information Security Management and Evaluation Competition - Phase II Answer Sheet" on their computer desktops after completion. The competitor's computer already has Office software installed and the necessary software tools (Tools kit) provided.

Tasks

Part I Response to network security incident

Task 1: Emergency response

Group A' web server has been hacked, the web application system of this server has been uploaded with malware and the system files have been corrupted by malware. Your team needs to help the company to trace the source of this cyber attack, conduct a comprehensive examination on the server, including log information, process information, system files, and malicious files, so as to analyze the hacking behavior, discover the system vulnerabilities, and fix them.

List of materials for this task: Server virtual machine.

The attacked server has been packaged as a whole and saved as a virtual machine file, so competitors are requested to import and analyze it independently.

Note: See the appendix for the basic configuration of the server. If it is not specified in the question, please use the default configuration.

Please complete the tasks for this section as required.

Task 1: Emergency response		
No.	**Task details**	**Answer**
1	Submit the attacker's two intranet IP addresses	
2	Submit the username and password of the website admin user	
3	Submit the time when the hacker gets the root account password of the mysql service (format: dd/MM/yyyy:hh:mm:ss)	
4	Find malicious code written by the hacker in WEB application files and submit the absolute file path	
5	Find the malicious code written by the hacker in the WEB application file and submit the code in its shortest form (format: <?php xxxx?>)	
6	Analyze the attacker's privilege escalation technique and submit the command through which the attacker successfully escalates the privilege	
7	Three absolute file paths associated with dynamic malware programs within the server	
8	The destination ip address of the malware's external connection	

Part II Digital forensics and investigation

Task 2: Malicious program detection in operating systems

A server system of Group A is infected with a malware, resulting in the destruction of key system files. Please analyze the system image and memory mirroring provided by Group A, find the malware in the system image, and analyze the malware behavior.

List of materials for this task: OS image, memory mirroring.

Please complete the tasks for this section as required.

Task 2: Malicious program detection in operating systems		
No.	**Task details**	**Answer**

1	Submit malicious process names (two)	
2	Location of corrupted files	
3	Memory address of encrypted data	
4	Original file content	
5	Analyze malware behavior	

Task 3: Network data packet analysis

Group A's network security monitoring system has discovered that malicious individuals are conducting an advanced persistent attack (APT) and some suspicious traffic packets have been captured. You are requested to search for clues of cyber attacks, decompose hidden malwares, and analyze the behavior of malwares based on the captured traffic packets.

List of materials for this task: Captured network data packet files.

Please complete the tasks for this section as required.

Task 3: Network data packet analysis		
No.	**Task details**	**Answer**
1	Submit malware transmission protocols (only one protocol should be submitted, those more than two are considered invalid)	
2	The destination ip address of the malware's external connection	
3	Name of the dll file loaded by the malware	
4	Decrypt the content of malware transmissions	
5	Analyze malware behavior	

Task 4: Computer standalone forensics

Analyze the given forensic mirror file, search for evidence keywords (clue keywords are "evidence 1", "evidence 2", ..., and "evidence 10", in text or image form, not case sensitive). Please extract and secure the subject evidence documents required by the competition, and fill in the relevant information according to the format requirements of the sample. The proportion of evidence documents in the total number of documents should not be less than 15%. Forensic information may be hidden in normal, deleted or damaged files, and you may need to apply code-conversion techniques, encryption and decryption techniques, steganography, data recovery techniques, and also be familiar with common file formats (e.g., office documents, compressed files and images).

List of materials for this task: Forensic mirror files.

Please complete the tasks for this section as required.

Task 4: Computer standalone forensics		
Evidence No.	**File name in the forensic mirror**	**Hash code of the original file in the mirror (MD5, not case sensitive)**
evidence 1		
evidence 2		
evidence 3		
evidence 4		
evidence 5		
evidence 6		
evidence 7		
evidence 8		
evidence 9		
evidence 10		

Part III Application security

Task 5: Android malware analysis

Group A has discovered that its published Android mobile application files have been illegally tampered with. Your team needs to assist Group A with reverse analysis of the malicious program sample, investigation and forensics of its attack/disruption.

List of materials for this task: Android APK files.

Please complete the tasks for this section as required.

Task 5: Android malware analysis		
No.	**Task details**	**Answer**
1	Submit the url address of the returned data from the malicious application in the material	
2	Submit the file name (including path) of the saved malicious code data in the material	
3	Submit SHA1 signature value of the dex initiated by the malicious behavior in the material	
4	Describe the behavior of the malicious code in the material	

Task 6: Malware analysis for the Windows system

Group A has discovered a malicious program is spreading in its network, and now that a sample of the malicious program has been collected, your team needs to assist Group A with reverse analysis of the malware sample, investigation and forensics of its attack/disruption.

List of materials for this task: Malware files.

Please complete the tasks for this section as required.

Task 6: Malware analysis for the Windows system		
No.	**Task details**	**Answer**
1	Submit the name of the function in the malware that implements the system attack	
2	Submit the system file name that the malware has attacked	
3	Submit the decryption key of the malware	
4	Describe the behavior of the malicious code in the material	

Marking allocation table:

Table 2 Marking Table for Phase II

No.	Description	Marking
B	Response to network security incidents, digital forensics and investigation, application security	
B1	Emergency response	
B2	Malicious program detection in operating systems	
B3	Network data packet analysis	
B4	Computer standalone forensics	
B5	Android malware analysis	
B6	Malware analysis for the Windows System	

Information Security Management and Evaluation Phase III

Network Security Penetration (CTF)

(Sample)

Test Projects for Competition in Phase III (Sample)

According to the technical requirements set forth in the information security management and evaluation, Phase III is network security penetration (CTF). This document contains the test projects for information security management and evaluation competition - Phase III.

The duration of the competition is 180 minutes.

Introduction

The objective of the CTF (network security penetration) is to implement network security penetration testing as a network security professional in a simulated network environment.

This module requires competitors, as the attacker, to complete penetration tests of the network using learned penetration testing techniques such as information collection, vulnerability discovery, and vulnerability exploitation; and to be able to analyze and obtain the existing Flag values using various information security related techniques.

Required Equipment, Machinery, Devices and Materials

All test projects can be completed by the competitors based on the equipment and software specified in the infrastructure list.

Marking Scheme

The marks for this project module is 30 points.

Description of Test Projects and Tasks

There are several servers in Group A's network, and each server hosts 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. Please see Appendix A for a sample network environment.

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
- Operating system vulnerability exploitation
- Miscellaneous and cryptographic analysis
- System file analysis

For the IP addresses of all devices and servers, see the list of devices provided on site.

Special Reminder

The marking is obtained by finding the correct flag value, which is shown in the following format:

flag{<flag value>}

This format may be hidden or even obfuscated in some circumstances. Therefore, pay attention to some sensitive information and find it out with tools.

Task

I. Portal

I. Portal			
Task No.	**Task description**	**Answer**	**Marking**
Task 1	There is hidden information in the enterprise portal, please find out the hidden information and submit the flag. flag format flag{<flag value>}		
Task 2	Enterprise portal is vulnerable, please penetrate the system, find and submit the flag. flag format flag{<flag value>}		
Task 3	Please obtain the package file in the root directory, analyze it and submit the flag. flag format flag{<flag value>}		

II. FTP server

II. FTP server			
Task No.	**Task description**	**Answer**	**Marking**
Task 4	FTP server is vulnerable, find and submit the flag in the FTP server. flag format flag{<flag value>}		
Task 5	Please obtain the package file in the FTP server, analyze it and submit the flag. flag format flag{<flag value>}		
Task 6	Please obtain the attachment in the FTP server, analyze the encrypted information in it, decrypt the content and submit the flag. flag format flag{<flag value>}		
Task 7	Please obtain the malicious files in the FTP server, analyze it and submit the flag. flag format flag{<flag value>}		

III. Enterprise mail server

III. Enterprise mail server			
Task No.	**Task description**	**Answer**	**Marking**
Task 8	Enterprise mail server is vulnerable, please penetrate the system and submit the flag stored in the backend of the system. flag format flag{<flag value>}		
Task 9	Please check the emails in the enterprise mail server, analyze the malicious files in the attachments, and submit the flag. flag format flag{<flag value>}		
Task 10	Please check the emails in the enterprise mail server, analyze the encrypted content in the emails, decrypt them and submit the flag. flag format flag{<flag value>}		

IV. Co-working server

IV. Co-working server			
Task No.	**Task description**	Answer	Marking
Task 11	Penetrate this backup server, find the flag file in the root directory, and submit the content as a flag. flag format flag{<flag value>}		
Task 12	Obtain the password plaintext for the root user and submit the plaintext as a flag. flag format flag{<flag value>}		

V. Single sign-on server

V. Single sign-on server			
Task No.	**Task description**	**Answer**	**Marking**
Task 13	There are hidden messages in the single sign-on server, please find out the hidden messages and submit the flag. flag format flag{<flag value>}		
Task 14	The single sign-on server is vulnerable, please penetrate the server and submit the flag in the database. flag format flag{<flag value>}		
Task 15	The backend of the single sign-on server is vulnerable, please penetrate the server and submit the content of the flag file in the root directory as a flag. flag format flag{<flag value>}		

VI. Application server

VI. Application server			
Task No.	**Task description**	**Answer**	**Marking**
Task 16	The running application on application server port 5555 is vulnerable, analyze it and submit the flag. flag format flag{<flag value>}		
Task 17	The running application on application server port 6666 is vulnerable, analyze it and submit the flag. flag format flag{<flag value>}		

Marking Distribution Table

Table 3 Marking Form for Phase III

No.	Description	Marking
C	CTF (Network security penetration)	
C1	Portal	
C2	FTP server	
C3	Enterprise mail server	
C4	Co-working server	
C5	Single sign-On server	
C6	Application server	

Appendix A

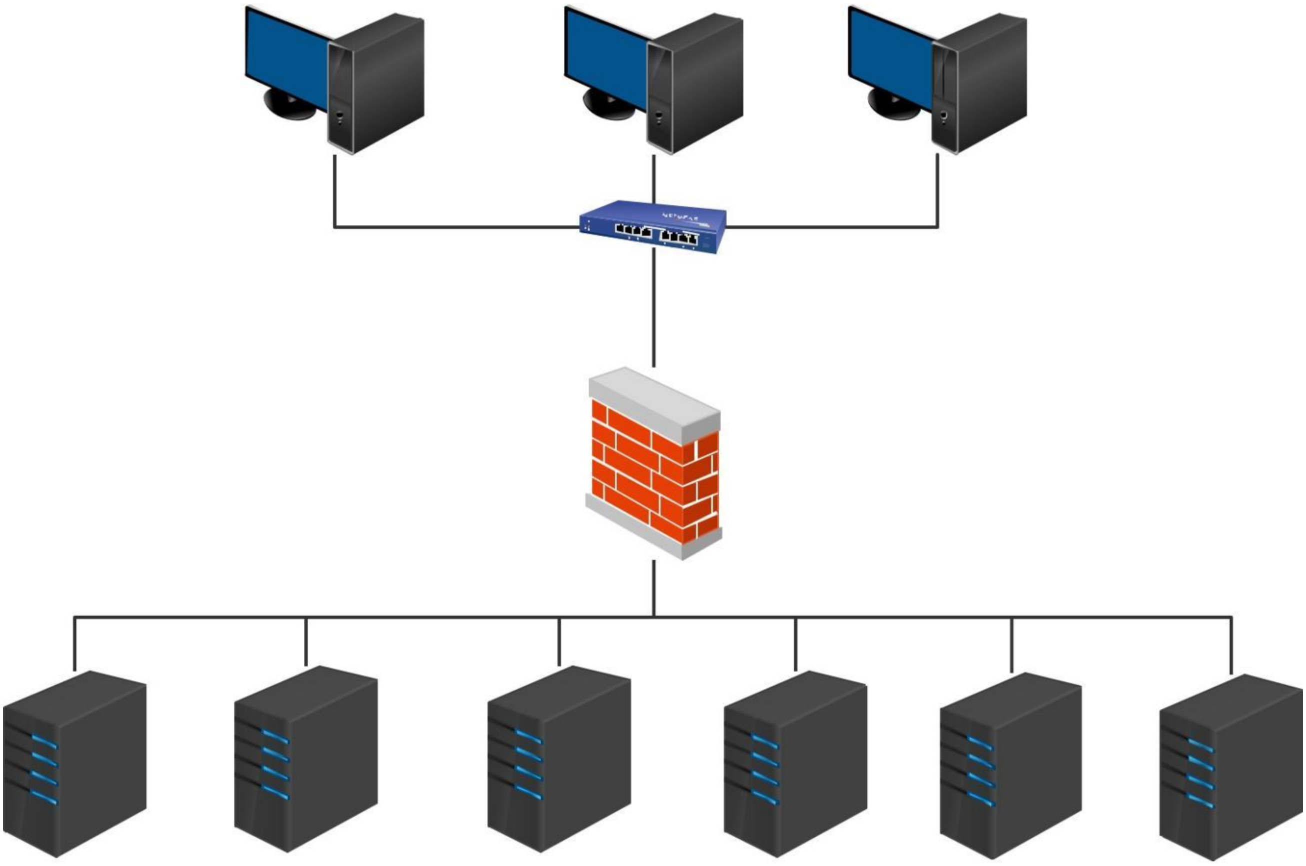


Figure 1 Network Topology Diagram