worldskills

Test Project

Cyber Security

CyberSecurity Incident Response, Digital Forensic Investigation and Application security

Submitted by:

Module B Group

Takayuki Terashima JP

Mohamed Saifulamri Omar SG

Andre Leopoldino de Souza BR

Xianzhi Lu CN

Anton Sergeev RU

Hung Leung HK

Contents

Introduction to Test Project

The following is a list of sections or information that must be included in all Test Project proposals that are submitted to WorldSkills.

- Contents including list of all documents, drawings and photographs that make up the Test Project
- Introduction/overview
- Short description of project and tasks
- Instructions to the Competitor
- Equipment, machinery, installations and materials required to complete the Test Project
- Other

Introduction

Warning: SAVE ALL YOUR CONFIGURATIONS!!! Every device will be rebooted before marking. The competition has a fixed start and finish time. You must decide how to best divide your time. **All answers to the Tasks must be written on the Answer Sheet provided in the Appendix.**

Please carefully read the following instructions!

Description of project and tasks

You and your team are the Group A network security technical support team. Wordpress on Group A's Webserver server was hacked on January 27, 2019. Your team needs to help Group A trace the source of this cyber-attack. Analyse the attack methods of hackers, find vulnerabilities in the system, submit an incident response report for cyber security incidents; Repair the vulnerabilities in the system, delete the backdoor hidden by the hacker in the system, and restore the normal operation of the system.

Task 1 Incident Response

Work Task Installation (Web_Server, File_Server, Competitor_01, Competitor_02)

Note: Please use the default configuration if you are not given the details; after the completion of the tasks in this section, fill in the "45th WSC2019 Cyber Security Project - Module B - Answer Sheet".

The base CentOS 7 has been set up on Web_Server , apache+mysql and wordpress web system has been installed; Windows Server 2012 OS has been set up on File_server; Windows 10 OS and other necessary Tools kits has been set up on Competitor_01 , Competitor_02.

Work Task Server Web_Server

Note: Please use the default configuration if you are not given the details.

- Linux Web settings see the appendix
- Incident Analysis
  - Find and submit the relevant commands and the parameters that is used in the attack.
  - Submit the time of the first attack.
  - Find and submit the filename of infected file in the web server used in the attack.
  - Find and submit the webshell code used in the attack.
  - Find and submit the malicious script of http tunnel
  - Find and submit the target IP of the http tunnel used in the attack.
  - Analyse how hacker get the credential and submit the modified password
  - Find and submit the path to the download file used by the hacker.

Work Task Server File_Server

Note: Please use the default configuration if you are not given the details.

- Windows settings see the appendix
- Incident Analysis
  - Find and submit the registry's string and the malicious filename used in the attack.
  - Find and submit the filename of self-starting malicious program used in the attack.
  - Analyse the self-starting malicious program and submit the process name and parameters used.
  - Analyse the malicious programs and submit any relevant hex signature strings contained in malicious programs

Work Task Competitor

- Fill in the cybersecurity incident response report

Task 2 Vulnerability Detection and Repair

Work Task Installation (Web_Server, File_Server)

Note: Please use the default configuration if you are not given the details; after the completion of the tasks in this section, fill in the "45th WSC2019 Cyber Security Project - Module B - Answer Sheet".

Work Task Server Web_Server

Note: Please use the default configuration if you are not given the details.

- Bug Fixing and Reinforcement
  - Modify PHP to forbid dangerous functions and submit changes made.
  - Modify Mysql's setting to limit the actions of importing and exporting and submit changes made.
  - Delete and submit the directory of the management tool on the web endpoint.
  - Fix the weak password issues
    - ✓ Submit the plain text of the weak password
    - ✓ Submit the URL of the pages with weak password
    - ✓ Submit the signature string "Passw0rd_******" on the feedback page after modifying the weak password (fill in the "*" part)

Work Task Server File_Server

Note: Please use the default configuration if you are not given the details.

- Bug Fixing and Reinforcement
  - Delete the malicious programs on the operating system and submit malware paths
  - Change the administrator password to the string in parentheses (AppServer123!@#) in CMD mode, and submit a screenshot after successful modification.
  - Deny access the 3389 port on the file_server, from web server

Task 3 Digital Forensic Investigation

Work Task Installation (LinuxM_Svr,Win.img, mem.dump, Network.pcap, Test.pdf, system.img)

Note: Please use the default configuration if you are not given the details; after the completion of the tasks in this section, fill in the "45th WSC2019 Cyber Security Project - Module B - Answer Sheet".

Work Task Server LinuxM_Svr

Note: Please use the default configuration if you are not given the details.

- Analyse malicious programs and recovery systems
  - Identify malicious program processes
  - Locate malicious program files
  - Analyse ELF files to describe their behaviour
  - Recover system settings modified by malware

Work Task Win.img, mem.dump

Note: Please use the default configuration if you are not given the details.

- Analyse malicious programs and recover files
  - Identify malicious program processes
  - Find hidden locations of malicious programs
  - Analyse PE files to describe their behaviour
  - Find the key left by malicious programs in memory
  - Recover files corrupted by malware

Work Task Network Analysis Network.pcap

Note: Please use the default configuration if you are not given the details.

- Analyse network packets
  - Identify malicious programs in network packets
  - Analyse PE files to describe their behaviour
  - Identify the target server for malicious programs
  - Analyse the network.pcap to find out what they are sending to the target server

Work Task Test.pdf, system.img

Note: Please use the default configuration if you are not given the details.

- Analyse malicious documents
  - Extract attack Payload
  - Analyse the Payload function
  - Recover lost files

Task 4 Code Review

Work Task Code Review

Review the code exhibits and answer the questions in Appendix accordingly. After the completion of the tasks in this section, fill in the "45th WSC2019 Cyber Security Project - Module B - Answer Sheet".

Specific Instructions to Competitors

Scenario

> As a senior software developer, code security is of utmost importance to you. It is part of your daily job to review codes developed by junior programmers. This is to ensure that the codes developed have no vulnerabilities. It is a daunting task at times because most of the codes are syntactically and semantically correct. You have to rely on your eye power and experiences to get you through.

You are required to carry out the following activities:

Each team will be given X code exhibits.

- Review each code exhibit and answer questions below as per in Appendix 1.
  - Identify the vulnerable line of code that poses a security threat.
  - Name the possible cybersecurity attack against the vulnerable code.
  - Explain how one can makes the code secure.
  - Provide the secure code (or line of codes) against the vulnerability.

Note: Observe and apply all safety rules and precautions

Appendix

Specification list

Web_#Server

organization:	Group A
Computer:	Web_Server
System username:	root
password:	W0rldskill@2019
IP address:	192.168.1.55/24

File_Server

organization:	Group A
Computer:	File_Server
System username:	Administrator
password:	W0rldskill@2019
IP address:	192.168.1.58/24

LinuxM_Svr

organization:	Group A
Computer:	LinuxM_Svr
System username:	root
password:	W0rldskill@2019
IP address:	192.168.1.59/24

Competitor_01

organization:	Competitor
Computer:	Competitor_01
System username:	Administrator
password:	123456
IP address:	192.168.1.252/24

Competitor_02

organization:	Competitor
Computer:	Competitor_02
System username:	Administrator
password:	123456
IP address:	192.168.1.253/24

Wordpress

organization:	Group A
Deployment path:	/home/wwwroot/default
Log path:	/home/wwwlogs/
URL:	http://192.168.1.55

Competition environment topology

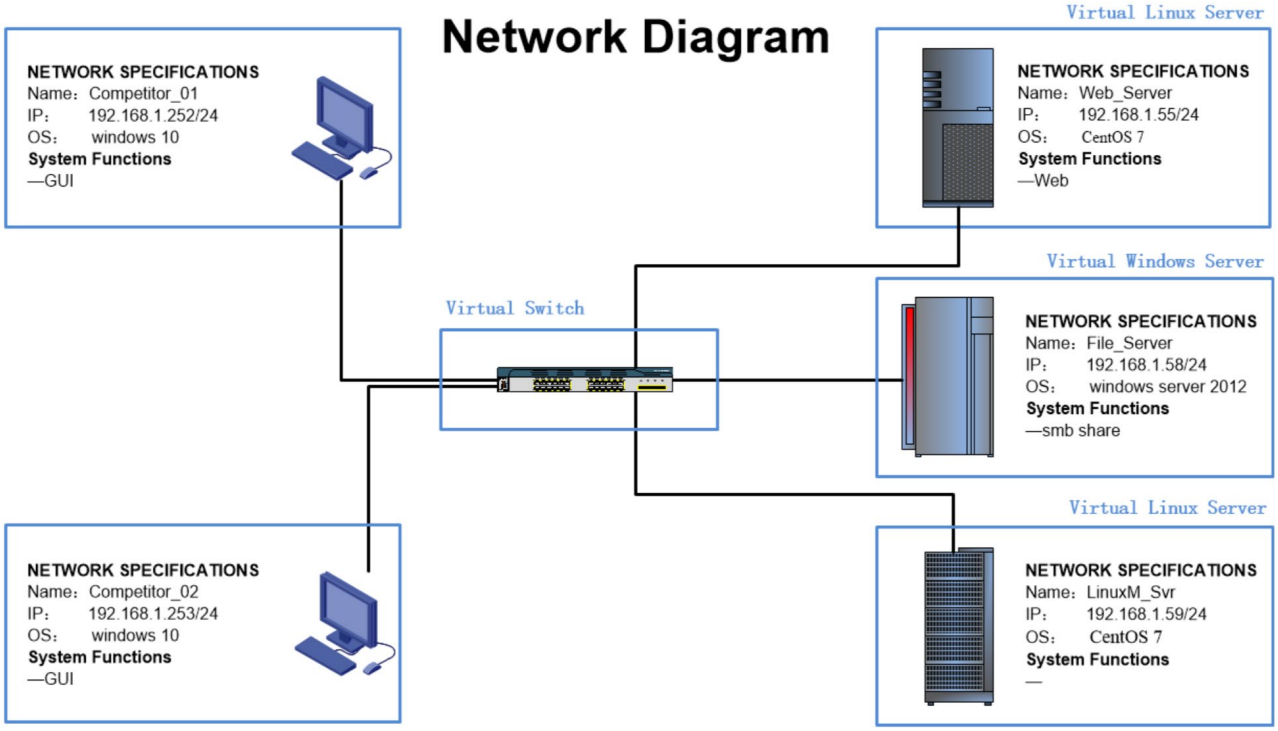

Figure 1 Module B competition environment topology

Answer Sheet

Task 1 Incident Response

45th WSC2019 Cyber Security Project - Module B - Answer Sheet

*Name:*_____

*Competitor No.:*_____

Work Task Server Web_Server

Tasks:	Answer:
Find and submit the relevant commands and the parameters that is used in the attack.	
Submit the time of the first attack.	YY / MM / DD : HH:MM :SS
Find and submit the filename of infected file in the web server used in the attack.	
Find and submit the webshell code used in the attack.	
Find and submit the malicious script of http tunnel	
Find and submit the target IP of the http tunnel used in the attack	
Analyse how hacker get the credential and submit the modified password	
Find and submit the path to the download file used by the hacker	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Work Task Server File_Server

Tasks:	Answer:
Find and submit the registry's string and the malicious filename used in the attack.	
Find and submit the filename of self-starting malicious program used in the attack.	
Analyse the self-starting malicious program and submit the process name and parameters used.	
Analyse the malicious programs and submit any relevant hex signature strings contained in malicious programs	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Work Task Competitor

Fill in the cybersecurity incident response report

Incident Report	Answer:
The harm and impact of this incident	
Safety corrective measures for this incident	
Remarks	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Task 2 Vulnerability Detection & Repair

45th WSC2019 Cyber Security Project - Module B - Answer Sheet

*Name:*_____

*Competitor No.:*_____

Work Task Server Web_Server

Tasks:	Answer:
Modify PHP to forbid dangerous functions and submit changes made.	
Modify Mysql's setting to limit the actions of importing and exporting and submit changes made.	
Delete and submit the directory of the management tool on the web endpoint.	
Fix the weak password issues	• Submit the plain text of the weak password • Submit the URL of the pages with weak password • Submit the signature string "Passw0rd_******" on the feedback page after modifying the weak password (fill in the "*" part)

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Work Task Server File_Server

Tasks:	Answer:
Delete the malicious programs on the operating system and submit malware paths	
Change the administrator password to the string in parentheses (AppServer123!@#) in CMD mode, and submit a screenshot after successful modification.	
Deny access the 3389 port on the file_server,from web server	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Task 3 Digital Forensic Investigation

45th WSC2019 Cyber Security Project - Module B - Answer Sheet

*Name:*_____

*Competitor No.:*_____

Work Task Server LinuxM_Svr

Tasks:	Answer:
Identify malicious program processes	
Locate malicious program files	
Analyse ELF files to describe their behaviour	
Recover system settings modified by malware	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Work Task Win.img, mem.dump

Tasks:	Answer:
Identify malicious program processes	
Find hidden locations of malicious programs	
Analyse PE files to describe their behaviour	
Find the key left by malicious programs in memory	
Recover files corrupted by malware	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Work Task Network Analysis Network.pcap

Tasks:	Answer:
Identify malicious programs in network packets	
Analyse PE files to describe their behaviour	
Identify the target server for malicious programs	
Analyse the network.pcap to find out what they are sending to the target server	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Work Task Test.pdf, system.img

Tasks:	Answer:
Extract attack Payload	
Analyse the Payload function	
Recover lost files	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Task 4 Code Review

45th WSC2019 Cyber Security Project - Module B - Answer Sheet

*Name:*_____

*Competitor No.:*_____

Code 1

Question	*Answer*
Identify the vulnerable line of code that poses a security threat.	
Name the possible cybersecurity attack against the vulnerable code.	
Explain how one can make the code secure.	
Provide the secure code (or line of codes) against the vulnerability. Note: There is no need to rewrite the whole code. Only the codes on the affected line will suffice.	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Code 2

Question	*Answer*
Identify the vulnerable line of code that poses a security threat.	
Name the possible cybersecurity attack against the vulnerable code.	
Explain how one can make the code secure.	
Provide the secure code (or line of codes) against the vulnerability. Note: There is no need to rewrite the whole code. Only the codes on the affected line will suffice.	

Note: All content in the report is required and is not allowed to be left blank. Where there is no content, replace it with the "-" symbol.

Please consult the diagrams and other additional information is provided in the appendix.