Test Project Cyber Security

Module B

CyberSecurity Incident Response, Digital Forensic Investigation and Application security

Submitted by:
Module B Group

Takayuki Terashima JP

Mohamed Saifulamri Omar SG

Xianzhi Lu CN

Dmitriy Serikov RU

Hung Leung HK

Renier van Heerden ZA

Joey Joseph Villota PH

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

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.**

You are expected to store the word document as PDF and named the file as country name. e.g Japan.pdf

We will provide necessary tools and challenge files on /share directory.

Please carefully read the following instructions!

Description of project and tasks

You are part of Network Security Technical Support team for Group A. The Webserver which is hosted by Group A, having Wordpress, was hacked on January 27, 2019. Your team has been called to help Group A for investigation and to 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 (report template available in the end of this Test Project); Repair the vulnerabilities in the system, delete the backdoor dropped by the hacker in the system, and restore the system to its normal operation.

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 otherwise; after the completion of the tasks in this section, fill in the "*45th WSC2019 Cyber Security Project - Module B - Answer Sheet*", which is available at the end of this test project.

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.

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 that the hack first executed the attack command
    - 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 name of webshell created by hacker
    - Find and submit the name of the function called by the webshell created by the hacker
    - Find and submit the target IP of the http tunnel used in the attack.
    - Submit the username and password that the hacker logged into the server with target IP of http tunnel

Work Task Competitor

- Fill in the cybersecurity incident response report available in the later pages of this test project document

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 i) pathname and ii) filename of the malicious program that locked your screen in the attack.
    - Submit the SHA1 checksum of the malicious program that locked your screen in the attack.
    - Find and submit the i) pathname and ii) filename of the stager program linked to the attack.
    - Enumerate the steps of the stager program in the attack.

Work Task Competitor

- Fill in the cybersecurity incident response report available in the later pages of this test project document

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 otherwise; after the completion of the tasks in this section, fill in the "**45th WSC2019 Cyber Security Project - Module B - Answer Sheet**" in the later section of this test project

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 otherwise.

- Bug Fixing and Reinforcement
  - Delete THREE malicious programs on the operating system and submit the i) pathnames and ii) filenames in the later section of this test project
  - 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 through the windows firewall (screenshot the firewall rule).

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 otherwise; 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 the system settings which were modified by malware (List the settings or provide the screenshot which were modified by the malware, Describe the steps, how to recover system)

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 the corrupted file by malware and then submit the file content.

Work Task Network Analysis Network.pcap

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

- You forgot to back up and have 10 bitcoins in your wallet, but the address and password are in a file that was encrypted by a ransomware.

Work task: dump_rev.pcap

- Identify and submit the key.

Work task: dump.raw

All you need is in the processes.

- Identify the malicious program process.
- Analyse PE files to describe their behaviour.
- Find the key and answer SHA1 checksum(task dump.raw).

Work task: dataenc.pcapng

If you got both keys in the previous files, you will be able to decrypt the file.

- Retrieve the file and submit the file content.

Work Task Test.pdf, system.img

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

- Analyse malicious documents
  - Extract malicious file, and submit the MD5 of malicious file
  - Decrypt the encrypted file, and submit the file content
  - Analyse the malicious file(payload).

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" in the later section of this test project.

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 3 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

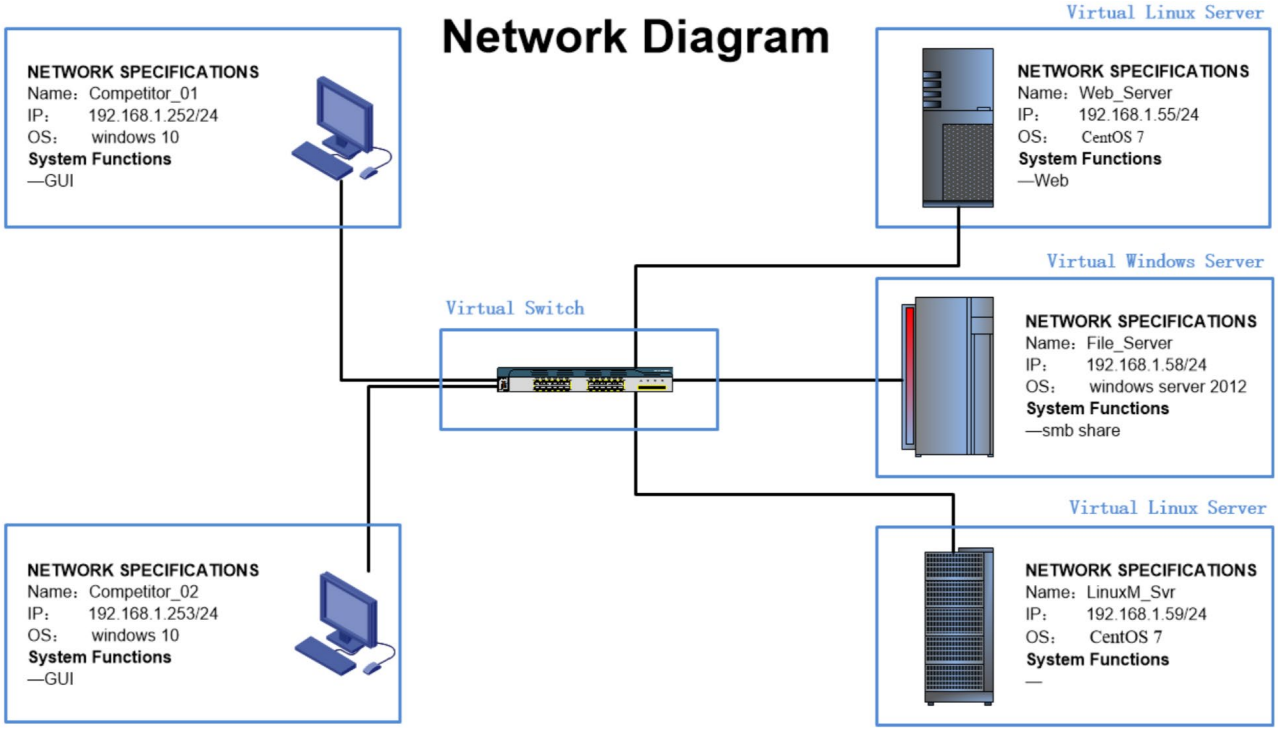

Figure 1 Module B competition environment topology

CODE REVIEW

Code 1

```
1	#include <stdio.h>
2	#include <stdlib.h>
3
4	void echo()
5	{
6		printf("%s", "Enter a word to be echoed:\n");
7		char buf[128];
8		gets(buf);
9		printf("%s\n", buf);
10	}
11
12	int main()
13	{
14		echo();
15	}
```

Code 2

```
1       #include <stdio.h>
2       int crack_code()
3       {
4               char code[10];
5               int val=999, i;
6               printf("Enter code: ");
7               gets(code);
8               for (i=0; i<10; i+=2)
9               {
10                      val = (val & code[i]) | code[i+1];
11                      val &= val >> code[i];
12              }
13              if (val == 101)
14              {return 0;}
15              else {return 1;}
16      }
17
18      void main()
19      {
20              if (crack_code()) {
21                      printf("Crack the secret code!\n");
22              }
23              else {
24                      printf("Now you know the secret!\n");
25              }
26      }
```

Code 3

Note: This is a PHP7 programming language

```
1       <?php
2
3       if( isset( $_POST[ 'btnSign' ] ) ) {
4               $message = trim( $_POST[ 'txtMessage' ]);
5               $name    = trim( $_POST[ 'txtName' ]);
6
7               $message = strip_tags( addslashes( $message ) );
8               $message =
mysqli_real_escape_string($GLOBALS["___mysqli_ston"],$message);
9               $message = htmlspecialchars( $message );
10
11              $name = str_replace( '<script>', '', $name );
12              $name = mysqli_real_escape_string($GLOBALS["___mysqli_ston"],$name);
13
14              $query  = "INSERT INTO guestbook ( comment, name ) VALUES
( '$message', '$name' );";
15              $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die(1);
16      }
17      ?>
```

Mark Summary Form

ID	Description	Mark Summary
B	**CyberSecurity Incident Response , Digital Forensics Investigation and Application Security**	**25.00**
B1	Incident Response:Work Task Server Web_Server	5.00
B2	Incident Response:Work Task Server File_Server	4.00
B3	Vulnerability Detection and Repair: Work Task Server Web_Server	1.50
B4	Vulnerability Detection and Repair: Work Task Server File_Server	1.50
B5	Digital Forensic Investigation: Work Task Server LinuxM_Svr	2.00
B6	Digital Forensic Investigation: Work Task Win.img, mem.dump	2.00
B7	Digital Forensic Investigation: Work Task Network Analysis Network.pcap	2.50
B8	Digital Forensic Investigation: Work Task Test.pdf, system.img	2.00
B9	Code Review: Work Task Code Review1	1.50
B10	Code Review: Work Task Code Review2	1.50
B11	Code Review: Work Task Code Review3	1.50

Answer Sheet

Task 1 Incident Response

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

*Name:*_____

*Country:*_____

*Workstation 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 that the hack first executed the attack command	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 name of webshell created by hacker	
Find and submit the name of the function called by the webshell created by the hacker	
Find and submit the target IP of the http tunnel used in the attack.	
Submit the username and password that the hacker logged into the server with target IP of http tunnel	

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:
Analyze the intrusion behavior and influence of hacker.	
What are the safety corrective measures for this incident?	

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 i) pathname and ii) filename of the malicious program that locked your screen in the attack.	i) pathname:
	ii) filename:
Submit the SHA1 checksum of the malicious program that locked your screen in the attack.	

Find and submit the i) pathname and ii) filename of the stager program linked to the attack.	i) pathname:
	ii) filename:
Enumerate the steps of the stager program in the attack.	

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	
What are the safety corrective measures for this incident?	

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:*_____

*Workstation 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 THREE malicious programs on the operating system and submit the i) pathnames and ii) filenames.	i) pathnames: filename:

	ii)	pathnames: filename:
	iii)	pathnames: filename:
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 through the windows firewall (screenshot the firewall rule).		

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:*_____

*Workstation 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 (Describe the steps, how to recover system)	

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 the corrupted file by malware and then submit the file content.	

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 and submit the key(dump_rev.pcap)	
Identify malicious program process.	
Analyse PE files to describe their behaviour	
Find the key and answer SHA1 checksum(task dump.raw)	
Retrieve the file and submit the file content.	

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 malicious file, and submit the MD5 of malicious file	
Decrypt the encrypted file, and submit the file content	
Analyse the malicious file(payload).	

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:*_____

*Workstation 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.

Code 3

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.