DCS22104 Fundamentals of Security in Ethical Hacking
Mock Midterm Examination Answer Script
January 2022

Section A (25 marks)

1. State five steps that can be done after a security breach. (10 marks)

   ✓ Learn from security breaches. Identify the security loopholes.
   ✓ Identify the severity of the damage. Compute the amount of loss of data.
   ✓ Setup a logger to monitor, if there is any future attack.
   ✓ Perform software updates. Software patches may fix certain security loopholes.
   ✓ Report to local authority or Interpol for security breach investigation.
   2 marks will be awarded for each correct step, up to five only.

2. Describe a malware in five statements. (10 marks)

   It is short for malicious software.
   It refers to computer virus.
   It is a malicious file which contains an executable file.
   It will not be executed unless it is opened by a user.
   It can infect any hardware and software platform.
   2 marks will be awarded for each correct statements above, other valid statement is also acceptable.

3. Discuss the differences between information and data, which become the goal point for the malicious parties. (5 marks)

   Information is a subset of data. (1 mark)
   Information contains human readable content. (2 marks)
   Data contains both human readable content and machine readable format. (2 marks)

Section B (25 marks)

1. Classify the following software applications in malicious versus impact table. (10 marks)

Calendar application	Internet relay chat (IRC)	Internet browser	Keylogger	Notepad
Spreadsheet	Text editor	Video call application	W32 worm	ZBot

	Non-malicious program	**Malicious program**
Harmless	Calendar application **(1 mark)** Notepad **(1 mark)** Spreadsheet **(1 mark)** Text editor **(1 mark)**	Keylogger **(1 mark)**
Harmful/ Catastrophic	Internet relay chat (IRC) **(1 mark)** Internet browser **(1 mark)** Video call application **(1 mark)**	W32 worm **(1 mark)** ZBot **(1 mark)**

2. Explain a hazard analysis in a software security. Then, name four debuggers and the corresponding programming languages. (10 marks)

It observes system states based on design constraints. **(2 marks)**

Debugger	**Programming language**	
JTest	Java	**(2 marks)**
Mocha	JavaScript	**(2 marks)**
C++ Unit Testing Framework	C++	**(2 marks)**
PHPUnit	Hypertext Preprocessor (PHP)	**(2 marks)**

3. Briefly analyze five weak points of a login system. (5 marks)

Password is visible. **(1 mark)**
Get method is used. **(1 mark)**
Script injection possible. **(1 mark)**
Password is reversible. **(1 mark)**
Fix token is used for a session. **(1 mark)**

Section C (25 marks)

1. State four basic query parameters that can be retrieved using a network enumerator. (4 marks)

Port number, services, state, domain name, and format of data segment.
1 mark will be awarded for each correct query parameter, up to four only.

2. Discuss the MOM strategy for photographing and give a suitable example scenario. (12 marks)

Strategy	**Discussion**	**Example scenario**
Method	Attack using an imaging device or a camera at the perspectives for certain scenes.	Using the built-in camera from a smartphone to take photos or videos.
Opportunity	It is convenience and able to share on the Internet almost immediately after captured.	Share a live feed on Facebook®.
Motive	Acquire photos or videos that contain visual scenes of certain importance.	Taking photographs of a company's trade secrets.

3. Write five lines of command to configure a server message block (SMB) service as shown in Table 1 in a given path "auxiliary/scanner/smb/smb_login". Verify the settings. (11 marks)

Table 1: Service settings

Parameter	**Value**
Host IP address	192.168.1.1
Thread	2
Port number	139
Username	Zacky

use auxiliary/scanner/smb/smb_login **(2 marks)**
set RHOSTS 192.168.1.1 **(2 marks)**
set THREADS 2 **(2 marks)**
set LPORT 139 **(2 marks)**
set USERNAME Zacky **(2 marks)**
show options **(1 mark)**

Section D (25 marks)

1. Define a software patch. Then, explain three purposes of a software patch (7 marks)
   It is a software updates. **(1 mark)**
   A program used to fix bugs for a software program. **(2 marks)**
   A program used to increase the usability for a software program. **(2 marks)**
   A program used to enhance performance for a software program. **(2 marks)**

2. State four advantages to practice the principle of least privilege. (8 marks)
   Prevent up to 90% of malicious code attacks. **(2 marks)**
   Difficult for malware to impact critical parts. **(2 marks)**
   Prevent non-administrative users from installing unknown programs. **(2 marks)**
   Allows security personnel to focus their efforts on fewer points of attack. **(2 marks)**

3. Explain five counter measures to protect a webserver in terms of environmental security. (10 marks)
   A server room should be running with good air ventilation to maintain in the room temperature. **(2 marks)**
   Extreme temperature; Too cool could slow down computer, while overheating could damage computer parts. **(2 marks)**
   A server room should be clean and tidy. **(2 marks)**
   Cable management and get rid of unused servers and its components. **(2 marks)**
   Technicians should be able to have enough space, such that they would not be confused or uncertain of which server to work with. **(2 marks)**

****