**Section A**

* Analyze the amount of loss after the breach
* Identify the loophole of the system that caused the breach
* Salvage remaining data that is untouched
* Reconfigure firewall rules of the system
* Check system loggers to identify the culprit
* ✓ 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.
* Malwares are malicious software that contain an executable file. The file does not execute by itself and only does when users open the file willingly.
* Malwares are either malevolent, benign or benevolent in nature. Some do not cause immediate damage to a computer system upon infection, while others cause catastrophic effects to computers instantly.
* Malwares can spread anywhere where sharing occurs. For example, worms are malwares that spread using communication protocols such as email, messenger and voice. Another example would be rabbits which reproduces and replicates itself inside multiple directories in a computer system to overload buffers.
* Malwares can be in anywhere in a computer system. It can be in your system directories, on your desktop or inside an application. They are well-hidden among important system files and they are usually difficult to spot at a glance.
* Malwares can be removed from volatile memory upon a complete system reboot. Malwares that live on in volatile memory such as RAM will be wiped out because they are only stored temporarily inside a system.

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.

3)

Data are unorganized attributes or characteristics that are results from a study. Information are organized facts of a study that are made from studying their collected data. Usually, malicious parties are more interested in collecting information as a goal point instead of data. This is because although information builds on data, these parties are more keen on getting the important bits of information rather than having a bunch of meaningless statistics that they need to organize later on. By collecting information, they can engineer various social engineering attacks using information that their victims would understand so that the victims realize about the severity of the situation and induce stress.

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**

|  |  |  |
| --- | --- | --- |
|  | Frequently used softwares (Non-malicious) | Unknown softwares (Malicious) |
| Harmless | Calendar application, Notepad, Text editor, Spreadsheet | Keylogger |
| Malicious | Internet relay chat (IRC), Video call application, Internet browser | W32 Worm, ZBot |

1. In a hazard analysis in software security, software should allow minimal inputs from the users. Software should also perform data validation. Lastly, software should increase its availability to each type of user. This is done so that script injection attacks are less likely to occur, and minimize the potential reason that drive unknown users to try and penetrate the system.

(It observes system states based on design constraints)

Four debuggers are:

- Mocha. Programming language: Java (JavaScript)

- JTest (Java)

- PHPUnit (PHP)

- C++ Unit Testing Framework (C++)

3)

- Poor data validation

- Poor authentication

- Predictable credentials

- Direct system object reference

- Poor error handling

-Password is visible

-Get method is used

-Password is reversible

-Script injection possible

-Fix token is used for a session

**Section C**

1. – Port numbers and their statuses

- ping sweep

- operating system version

- Trace route table

-Port number, services, states, domain name, format of data segment

**2.**

|  |  |  |
| --- | --- | --- |
| **Strategy** | **Discussion** | **Example** |
| Method | Attack using an imagery device in the perspectives of the victim | Using built-in camera of victim computer to take photos of victim’s activity |
| Opportunity | Convenient and able to share acquired photos instantly to the Internet | Share live feed on Facebook |
| Motive | Able to obtain visual information of certain importance | Able to obtain company trade secrets |

**3.** 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**

1. A software patch is a software update that aims to fix software vulnerabilities that are previously found. A software patch aims to:

- Ensure the integrity of software files. It helps repair corrupted software files if any.

- Ensure the performance of the software. It removes any unnecessary files that are no longer in use and ensures smooth software performance.

- Prevent undocumented backdoors from infecting client computers. It removes any malicious files that have been introduced unknowingly and prevents users from introducing them to their own computers.

-fix bugs of a software program

-increase usability of software program

- increase performance of software program

2.

-Malicious parties have lesser options to conduct an attack.

-Less possibilities to consider when identifying the culprit.

-Reduce management oversights.

-Ensure the confidentiality of company secrets. Employees of a company will have less knowledge of company secrets if their privileges are limited to what their job scope requires.

-prevent up to 90% of malicious code attacks

-difficult for malware to impact critical parts of system

-prevent unauthorized users from installing unknown programs

-Allows security personnel to focus their efforts on fewer points of attack

3.

-Server room should have good air ventilation and maintaining room temperature.

-Extreme temperature, damage computer parts, cool temperature impact and slows down performance

-Server room dust free, pest-free, clean and tidy.

- Good cable management, get rid of unused servers and its components

- Technicians have enough space to work with, they should not be too confused or uncertain about the functions of each server.