**Class Assignment 01**

**Cyber Forensics**

**Date of Assignment**: 8th August 2024

**Last Date of Submission**: 30th August 2024

**Length of answer**: 3000 words max / question

**Question No. 1**

In theory, you learnt the five types of hacker threats that are common on the internet: commodity threats, hacktivists, organised crime, espionage and cyberwar. In Assignment 1, you are required to choose any three of the five types of hacker threats and undertake some research into the cybersecurity literature and/or media coverage to find one incident for each of the chosen three types of hacker threats. For each incident, you will:

1. describe the attack and the immediate result of the attack (i.e. what was the asset that was  
compromised?)

2. describe the motivation behind the attack

3. identify and describe the vulnerability (or vulnerabilities) in the organisation that made the attack possible

4. describe the short-term and long-term impact (financial, reputational or otherwise) of the attack on the organisation

5. describe the responses from the affected organisation and society as a whole.

Reflect on all the incidents, and critically discuss the factors that make the prevention of cyber-attack challenging.

The incidents should meet the following criteria:

• The attack must be a cyber-attack.

• The attack was within the last ten years.

**Question No. 2**

1. **How to shut down a Linux system?**
2. **What is Halt and power off command in Linux?**
3. **How to change the password of a user in Linux System. Explain with an example.**
4. **How to show hidden files in Windows XP and Windows 2003 Explain with an example.**
5. **Versions of MS-Windows Operating Systems for PCs.**
6. **What is kernel in Linux OS?**
7. **What is Terminal Mode in Linux? What is the meaning of # and $ in terminal?**
8. **Explain about the File permission in Linux in details.**
9. **Explain how to Format a hard disk and loading Operating System.**

Here are the answers to your questions grouped by topics:

### Question No. 1: Types of Hacker Threats and Incidents

You'll need to conduct your own research to find specific incidents that meet the criteria of being within the last ten years and relating to the three types of threats you choose. I can guide you on how to proceed:

1. \*\*Select three types of hacker threats:\*\* For example, choose commodity threats, hacktivists, and organized crime.

2. \*\*Research incidents:\*\* Look for well-documented cyber-attacks for each type in cybersecurity literature or media. Google Scholar, cybersecurity blogs, and news websites are good starting points.

3. \*\*Analyze each incident:\*\* For each selected incident, describe the attack, the compromised asset, the motivation, the vulnerabilities exploited, and both the short-term and long-term impacts. Also, detail the response from the affected organization and the broader societal reaction.

4. \*\*Reflect on the challenges:\*\* Discuss the common factors across the incidents that make preventing cyber-attacks challenging, such as technological complexity, human factors, or regulatory issues.

### Question No. 2: Linux and Windows System Commands and Concepts

a) \*\*How to shut down a Linux system?\*\*

- To shut down a Linux system immediately, you can use the command:

```

sudo shutdown now

```

- To schedule a shutdown:

```

sudo shutdown -h +time

```

Replace `+time` with the number of minutes (e.g., `+10` for ten minutes later).

b) \*\*What is Halt and power off command in Linux?\*\*

- `halt`: This command stops all CPUs on the system but does not necessarily power off the machine.

- `poweroff`: This is effectively the same as running `halt` but with the poweroff flag, ensuring the system actually turns off.

c) \*\*How to change the password of a user in Linux System.\*\*

- To change a user's password, use:

```

sudo passwd username

```

Replace `username` with the actual user's name. Follow the prompts to enter a new password.

d) \*\*How to show hidden files in Windows XP and Windows 2003\*\*

- Open Windows Explorer.

- Go to Tools > Folder Options > View tab.

- Check "Show hidden files and folders."

- Example command in the command prompt:

```

dir /A:H

```

e) \*\*Versions of MS-Windows Operating Systems for PCs\*\*

- Windows XP

- Windows Vista

- Windows 7

- Windows 8/8.1

- Windows 10

- Windows 11

f) \*\*What is kernel in Linux OS?\*\*

- The kernel is the core part of the Linux operating system, managing the system's resources and the communication between hardware and software components.

g) \*\*What is Terminal Mode in Linux? What is the meaning of # and $ in terminal?\*\*

- Terminal mode is a text-based interface in Linux where users enter commands.

- `#` symbolizes the root user prompt, indicating administrative privileges.

- `$` indicates a normal user prompt without administrative privileges.

h) \*\*Explain about File permission in Linux in details.\*\*

- Linux file permissions dictate who can read, write, and execute a file.

- Permissions are shown as `rwx` where `r` stands for read, `w` for write, and `x` for execute.

- Permissions are defined for three types of users: owner, group, and others.

i) \*\*Explain how to Format a hard disk and loading Operating System.\*\*

- \*\*Formatting a hard disk:\*\*

- Use a tool like `fdisk` or `gparted` to partition the disk, then format partitions using a file system (e.g., ext4 for Linux).

- \*\*Loading an Operating System:\*\*

- Boot from an installation media (USB/DVD).

- Follow the OS installation prompts to install on the formatted hard disk.

These are basic guidelines and commands; for detailed usage and options, the man pages (`man command-name`) in Linux provide comprehensive information.