Computer Forensic & Investigation

Lab2: Exercise

THE 21ST CENTURY MODERN ATTACK.

There are many ways to categorize computer crimes. In chapter 1, you have seen a history of computer crime and types of computer crime in this century. You might divide them according to who commits them and what their motivation might be (e.g., professional criminals looking for financial gain, angry ex-employees looking for revenge, crackers looking for intellectual challenge). Or, you might divide these crimes by how they are perpetrated (e.g., by physical means such as arson, by software modifications, etc.).

In this activity, we have chosen to give you a fuller understanding of computer crimes by the types of computer security that ought to prevent them. Within your group, explain in detail each of the following area:

1. **Privilege Escalation**
2. **Malware**
3. **Phishing**
4. **Social Engineering**
5. **Session Hijacking**
6. **Password Cracking**
7. **Denial of Service Attack.**

The objectives of this assessment item are to develop capabilities in:

- organisational and cooperative skills
- researching a topic and sharing the results
- lifelong learning & critical capabilities in information management

within the context of developing a background general knowledge of important issues in computer forensics. This presentation will be assessed by the class as a whole as well as by the co-ordinator, lecturers and any other interested attendees.

End of Lab2