Computer Forensic & Investigation

Lab1: Computer Crime Analysis

Practical 1 – Week 1 & 2

The lecture discussed that computer crimes could be characterised according to the following headings:

- Motive
-
- target
- skill level
- type of computer security incident
- role of the computer
- insider / outsider

Groups of 3 or 4 people will analyse a number of cases from the US Department of Justice Cybercrime Cases site:
Eg: http://www.justice.gov/opa/pr/2013/January/

Group	Year	Links
1	2014	http://www.justice.gov/opa/pr/2014/February/14-tax-205.html
2	2013	http://www.justice.gov/opa/pr/2013/March/13-tax-357.html
3	2015	http://www.justice.gov/opa/pr/seven-individuals-indicted-multimillion-dollar-business-opportunity-fraud-scam
4	2011	http://www.justice.gov/opa/pr/2011/November/11-crm-1534.html
5	2010	http://www.justice.gov/opa/pr/2010/December/10-crm-1453.html
6	2009	http://www.justice.gov/opa/pr/2009/January/09-at-061.html

Answer the following questions.

1. Give a brief description of the case.
2. What are the characteristics of the case? In some of these cases, there is insufficient detail in the case note to classify all characteristics.
3. If reported, what were the sources of computer evidence in the case?

Discuss the case amongst the group.
Divide the questions among the group.
Present answers to the class.

Computer Forensic & Investigation

Lab1: Computer Crime Analysis

Characterization of Computer Crimes

Motive

Chapter 1 of Mohay et al discusses a range of motives that have been suggested for computer crime. These include but are not limited to:

- financial gain
- mischief or harm
- intellectual challenge
- convenience

Please note that this list of motives may be inadequate. Feel free to add to the list.

Target

The following breakdown of target classes may be used:

- government
- financial institution
- IT-related company
- other corporate
- educational institution
- individual – known to perpetrator
- individual – unknown to perpertrator

This set of targets may be inadequate. Add to the list if necessary.

Skill Levels

The following list of skill levels may be used:

- elementary level (desktop user, web search, email)
- experienced user level (elementary plus daily workplace experience)
- intermediate level (experienced user, some programming and operating system expertise)
- high level (professional IT worker)
- hacker level (intensive study and experience)

Type of Security Incident

The SANS article *Computer Forensics – An Overview* (D. Lunn) suggests the following major headings for computer security incidents:

- virus attack
- unauthorised access
- information theft or confidentiality loss
- attacks against system functionality
- denial of service attack

- information corruption

Role of the Computer

As suggested in Chapter 1 of Mohay et al, IT resources can play three different roles (possibly more than one at a time) in a computer related crime:

- the computer is utilized as a tool for perpetrating cybercrime
- the computer is used as a target of the cybercrime
- the computer is used as a repository for storing information related to the cybercrime being perpetrated

Insider/Outsider

While computer crime reports in the press support the public view that everyone is under threat from anonymous cyber-terrorists, computer security specialists continue to assert that up to 90% of computer related crimes are committed by “insiders”. The following categories may be used in your analysis:

- outsider (no known connection with target)
- insider with special privilege (e.g. system administrator)
- insider with normal privilege (e.g. workplace user)
- ex-employee retaining privileges

End of Lab1