Mediums used to spread content related incidents

There are various mediums used in spreading or propagating content related incidents on the net. Most of the mediums used for content related incidents between January to June 2011 are as follows; 23 incidents were recorded via websites followed by eight (8) incidents via social networking sites, five (5) incidents via blogs/forums, three (3) incidents via emails, two (2) incidents via videos and one (1) incident via mobile phone.

Examples of Incidents

Issues defined as national threat in the first half of 2011 were insulting Prophet Muhammad, insulting Malaysia/ Malaysians and insulting the people of Sarawak. Any blogs or websites that had been created for the purposes of insulting a particular religion or group of people on the Internet could potentially create havoc in the real world.

An interesting incident in first half of 2011 is related to pornography in a social networking site called Facebook. Facebook users got a link through their private chat that contains a pornographic video. Once these Facebook users clicked on the link, all of their friends in their list received the link through their private chat as well. Upon investigation, it was a malicious domain that redirected users to a Facebook application which allowed the application to access these users' chat and spammed their friends.

Intellectual property incidents that occurred during the same time period mostly took place when an unauthorised party replicated a website that belonged to someone else. The purpose of replication is to scam Internet users to believe that the site is a valid website. Later, the scammer may ask for money or personal information from Internet users.

Recommendation

MyCERT advise Internet users to be extra careful when posting any type of content on the Internet. They particularly must not post any offensive content that could spark hatred towards a person or a group of people. We also advise Internet users to report to Cyber999 if they are faced with any offensive content such as pornography and national security threats on the net.■

References

1. http://en.wikipedia.org/wiki/Intellectual_property

2. MyCERT Definitions of Incidents and SLA

3. CMCF website - http://www.cmcf.my/fact-sheet

Vulnerability Analysis Using Common Criteria Attack Potential (Part 2)

By | Ahmad Dahari Bin Jarno

Part 1 Continuity - Abstract

In part one (1) of this article, discussion on Common Criteria and several other Vulnerability assessments, including Penetration testing Methodologies, were elaborated in extreme detail. It must be noted that each methodology existed as in individual forms, which are not yet perfect, thus insignificant in providing a better justification in situations concerning vulnerability analysis processes and results.

Therefore, further studies were carried out on Common Criteria (CC) specifically on Attack Potential. This is part of the work unit requirements of CC evaluation process, providing guidance, steps and the flow of vulnerability assessments/ penetration testing processes. In addition, it also accommodates the analysing of vulnerabilities found during assessments.

Such approaches introduced by CC make vulnerability assessments analysis more valuable and significant in providing better justifications with respect to its assessments. To achieve this, adapting CC Attack Potential in current vulnerability assessments/penetration testing methodologies are recommended to provide better value in executing Security Assessments . Part two (2) of this article will further discuss this matter.

Requirements	OSSTMM	NIST	OWASP	Pen-Test FW
1. Planning Phase	High Level Understanding Only. Depends on VA Analyst Capabilities	Have and described in detail	No details provided	No details provided
2. Execution Phase	High Level Understanding Only. Depends on VA Analyst Capabilities	Have and described in detail	Flows of process is described but not in detail	Flows of process is described but not in detail
3. Details of Approaches	High Level Understanding Only. Depends on VA Analyst Capabilities	Have and described in detail	Have and described in detail	Have and described in detail
4. Applicability in all scenarios/ technologies	Partly applicable. Fill in the Blank Forms	Focus on Network	Only for Web Apps Assessment	Focus on Network
5. Categorising findings	High Level Understanding Only. Depends on VA Analyst Capabilities	Yes but only specific for Network	Yes but only Web Apps and Implementations related	Yes
6. Analysis Findings	High Level Understanding Only. Depends on VA Analyst Capabilities	Yes	No details provided	Partially
7. Risk Analysis	No details provided	No details provided	No details provided	No details provided
8. Reporting in detail	Partially, depending on clients' requirements client	Yes	Partially	Partially

Table 1: *List of Requirements Applicability of Vulnerability assessments/Penetration testing methodologies.*