Penetration Testing Model for Website Hosted in Nuclear Malaysia

By Mr Mohd Dzul Aiman bin Aslan, Mr Mohamad Safuan bin Sulaiman, Pn Siti Nurbahyah binti Hamdan, Mr Saa'idi bin Ismail, Mr Mohd Fauzi bin Haris, Pn Norlelawati, Pn Norzalina binti Nasiruddin, YM Raja Murzaferi Mokhtar,
Pusat It,
Agensi Nuklear Malaysia

Structure of Presentation

1. **Introduction**
2. **Objective**
3. **Methodology**
4. **Result and Conclusion**
5. **Future work**

1. Introduction

Penetration Testing

What is penetration testing?
A penetration test is a **method of evaluating the security of a computer system or network by simulating an attack** from malicious **outsiders** and malicious **insiders**.

Why do we need to perform penetration testing on our own website?

1. Introduction

Website

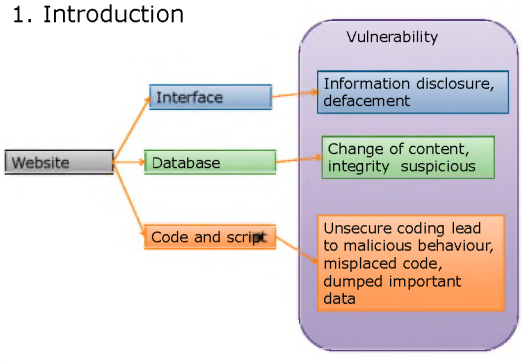
-Impose a 'picture' of an individual, organisation, country

- Confidence to customer on their core business

- Nuclear Malaysia has a quiet a number of websites internal and external (internet)

- There are nine internet-based application hosted are on Nuclear Malaysia website

1. Introduction



2. Objectives

-To build a penetration testing model for website hosted in Nuclear Malaysia

- To strengthen website security against cyber threats

- To protect against malicious attempts and information disclosure

3. Methodology

Methodology of Penetration Testing Manual:

-OSSTMM (Open Source Security Testing Methodology Manual) - ISECOM

-NIST (National Institute of Standard and Technology) – US Department of Commerce

- ISSAF (Information Systems Security Assessment Framework) - OISSG

Methodology

1. Objective and Scope of testing

URL: domain or subdomain

Obtain permission from respective owner (legality)

Define objectives and scope

Time, duration and resources and etc.

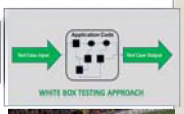
http://sp-kms.nuclearmalaysia.gov.my/Pages/Home.aspx

Methodology

2. Testing Approach

Blackbox — Don't have preliminary knowledge of the targeted system. Simulate outsider

Whitebox — Have some knowledge of the targeted system. Simulate insider



Methodology

3.0 Running the test:

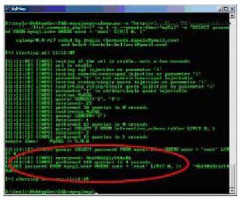
3.1 Website : SQL Injection, XSS, CSRF, misplaced dump, misplaced configuration file

- Example tools: Acunetix, Pangolin, Metasploit Farmework, Havij

Methodology

3.2 Database : prediction for table, blind SQL injection

- Example tools: SQLninja, SQLmap



Methodology

3.3 Known vulnerability for specific package : Joomla vulnerability, Sharepoint vulnerability

- Example advisory: Joomla advisory, Sharepoint Hacking Diggity Project, packetstorm security, exploit database, Inj3ct0r

Methodology

Top Ten Open Web Application Security Project (OWASP)

OWASP	OWASP Top 10 – 2010 (New)
	A1 – Injection
	A2 – Cross-Site Scripting (XSS)
	A3 – Broken Authentication and Session Management
	A4 – Insecure Direct Object References
	A5 – Cross-Site Request Forgery (CSRF)
	A6 – Security Misconfiguration (NEW)
	A7 – Insecure Cryptographic Storage
	A8 – Failure to Restrict URL Access
	A9 – Insufficient Transport Layer Protection
	A10 – Unvalidated Redirects and Forwards (NEW)

Methodology

4.0 Result

Result of te

Suggestion

- Based on Malaysia an

Treatment s programme

Document Grinding (Electronic Dumpster Diving)

The parameter here is important in the verification of much of the tested inf
of what is considered information security. The amount of time granted to t
information is dependent upon the size of the organisation, the scope of the
planned for the testing. More time however, does not always mean more in
to key pieces of the security puzzle.

Expected Results	(see Appendix E for the default template) A profile of the organization A profile of the key employees A profile of the organization's network

Tasks to perform for a thorough Document Grind:

- Examine web databases concerning the target organization and key pe
- Verify key persons to personal homepages, published resumes, and or
- Compile e-mail addresses from within the organization and personal e-
- Search job databases for skill sets technology hires need to possess in
- Search newsgroups for references to and submissions from within the
- Search documents for hidden codes or revision data.

Document Grinding (Electronic Dumpster Diving)

The parameter here is important in the verification of much of the tested information and pertains to many levels of what is considered information security. The amount of time granted to the researching and extraction of information is dependent upon the size of the organisation, the scope of the project, and the length of time planned for the testing. More time however, does not always mean more information but it can eventually lead to key pieces of the security puzzle.

Expected Results	(see Appendix E for the default template) A profile of the organization A profile of the key employees A profile of the organization's network

Tasks to perform for a thorough Document Grind:

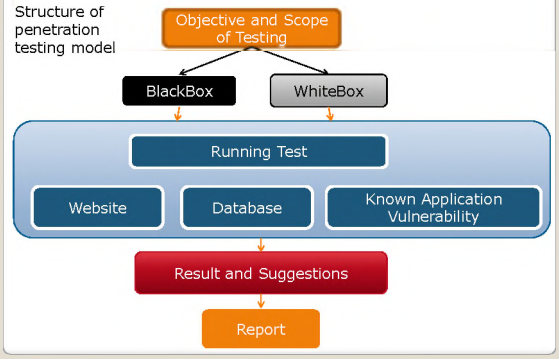
- Examine web databases concerning the target organization and key people.
- Verify key persons to personal homepages, published resumes, and organizational affiliations.
- Compile e-mail addresses from within the organization and personal e-mail addresses from key people.
- Search job databases for skill sets technology hires need to possess in the target organization.
- Search newsgroups for references to and submissions from within the organization and key people.
- Search documents for hidden codes or revision data.

5.0 Report

Report will consist of technical report and summary of the penetration testing conducted and recorded for future reference.

Result and Conclusion

Structure of penetration testing model



Result and Conclusion

Sample of penetration testing has been done to following website based on their specific objective:

-Nuclear Malaysia main website (http://www.nuclearmalaysia.gov.my)

- Nuclear Malaysia Sharepoint main website (http://sp-kms.nuclearmalaysia.gov.my)

With this penetration testing model and methodology conducted, customers and users will gain confidence in security of Nuclear Malaysia website.

Future work

As new treats and attack vector keep arising everyday along with technology, an updated version of knowledge must be applicable on conducting the test.

Enhancement on the techniques of test (attacking techniques).

It is suggested that all Nuclear Malaysia website tested using above methodology and periodically.

Revision of model to satisfy with government policy and standards.