PKF Avant Edge

MSC MALAYSIA Status Company

PKF

Penetration Testing

Stevie Heong – CISSP, CISA, CISM, CGEIT, CCNP

What is Penetration Testing (PenTest)?

▪A way to identify vulnerabilities that exists in a system/network that has existing security measures in place

▪Answers the questions on whether your IT security is strong enough

▪Attacking methods conducted by trusted individuals, that are used similarly by hostile hackers

▪PenTest done in stages: Discover, Analyse, Validate, Exploit and Report.

▪PenTest is a snapshot of a company's security posture with specific time frame

▪PenTest is NOT a full security audit or a compliance audit, although it might be used in one, for example ISO27001 implementation

▪PenTest is used to either

a) Increase upper management awareness of security issues
b) Test intrusion detection and response capabilities
c) Assist management in decision making process to prioritise critical fixes

Consequences of PenTest

- Improper Pentest can cause:

a) Network congestion
b) Systems outages and downtime
c) DDOS on web applications
d) Blockage of legitimate traffic
e) Total destruction of data
f) Management panic
g) Technical Crisis
h) Brand Dilution
i) Customer complaints
j) Business Continuity Problems

✓ Vital to have management consent before proceeding!

✓ Vital to set RoE (Rules of Engagement)

Types of PenTest

Black Box Penetration Testing

- zero-knowledge testing
- Tester need to acquire the knowledge and penetrate.
  - Acquire knowledge using tools or Social Engineering techniques
  - Publicly available information may be given to the penetration tester,

Benefits:

Black box testing is intended to closely replicate the attack made by an outsider without any information of the system. This kind of testing will give an insight of the robustness of the security when under attack by script kiddies

Types of PenTest

White Box Penetration Testing

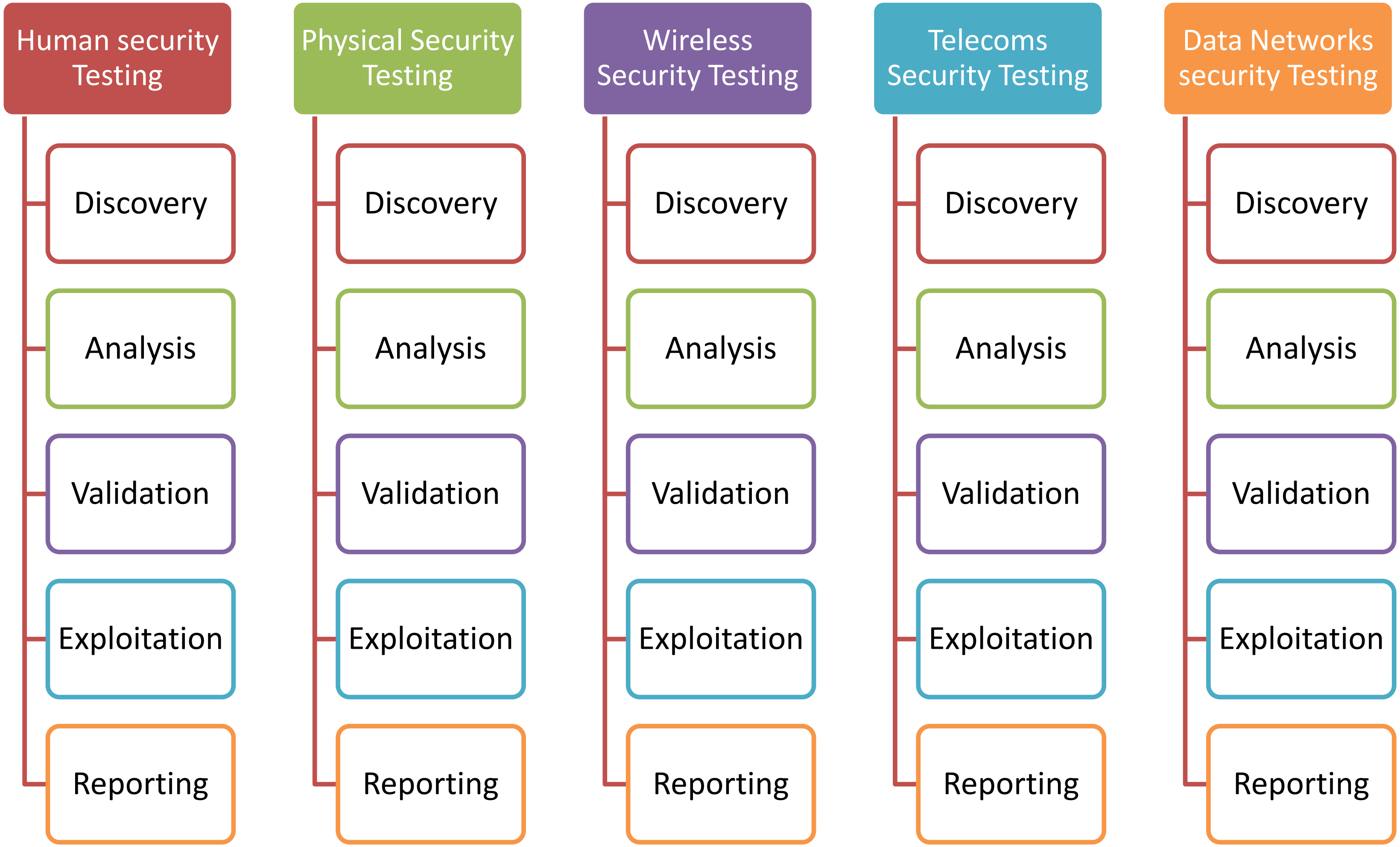
- complete-knowledge testing
  - Testers are given full information about the target system they are supposed to attack .
    - Information includes ,
      - » Technology overviews,
      - » Data flow diagrams
      - » Code snippets
      - » More…..

Benefits:

- reveals more vulnerabilities and may be faster.
- compared to replicate an attack from a criminal hacker that knows the company infrastructure very well. This hacker may be an employee of the company itself, doing an internal attack

AvantEdge PenTest Methodology

We use the OSSTMM (Open-Source Security Testing Methodology Manual) methodology:



Human security Testing
- Discovery
- Analysis
- Validation
- Exploitation
- Reporting

Physical Security Testing
- Discovery
- Analysis
- Validation
- Exploitation
- Reporting

Wireless Security Testing
- Discovery
- Analysis
- Validation
- Exploitation
- Reporting

Telecoms Security Testing
- Discovery
- Analysis
- Validation
- Exploitation
- Reporting

Data Networks security Testing
- Discovery
- Analysis
- Validation
- Exploitation
- Reporting

Discovery Phase

We can either discover the IP addresses or be provided the IP address range for the network to be reviewed by us.

Examples of Network IP Addresses:

□ 192.***.***.157
□ 192.***.***.24
□ 192.***.***.25
□ 192.***.***.26
□ 192.***.***.27

We will use the our security tools to identify live services on the tested host on this subnet. These tools are designed to identify live systems, as well as services being offered by those systems.

Analysis Phase

As a follow-up to the information gathered, we will then use the security tools like Nessus and Metaspoilt to perform checks for known vulnerabilities on the external network.

These tools are security-scanning tools that check for thousands and thousands of different known vulnerabilities on networked systems. For instance, the Nessus tool performs extensive checks for vulnerabilities based upon predefined attack signature criteria.

All tests are then complemented with additional manual checks performed by our certified PenTest engineers to ensure accuracy of the results.

Validation Phase

In this phase, we will manually verify the outputs of all security tools to determine if any results are inconsistent and warranted additional examination and review.

Outputs from the various tools used will be compared and crosschecked for accuracy.

False positives and duplicate entries will be removed from the Investigation results.

Vulnerabilities that could be neither confirmed nor disputed are categorized separately for follow-up checks and review.

Those vulnerabilities that could not be tested and confirmed without endangering the systems on which they exist are noted as well.

Exploitation Phase

This is where the rubber meets the road.

We will perform exploitation attempts against any external network host exhibiting vulnerability symptoms.

These attempts include numerous manual exploitation attempts, information gathering and password guessing for well-known accounts using techniques developed and tested in our lab environment.

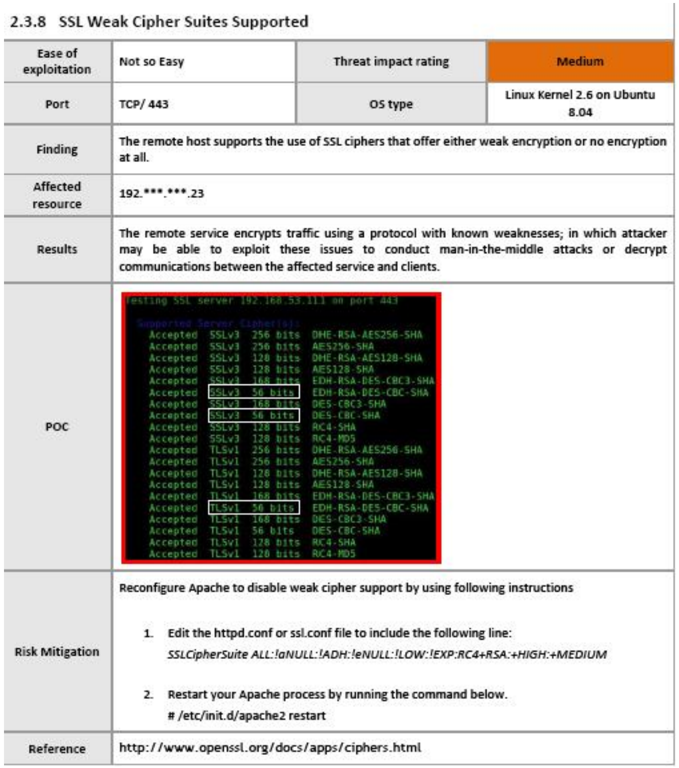
All attacks are designed to limit the danger to services on the systems in order to prevent disruption of service during the testing.

Reporting Phase

- Organize Data/related results for Management Reporting
- Consolidation of Information gathered
- Analysis and Extraction of General conclusions
- Recommendations.

Overall Structure of our report as follows:

▪Executive summary
▪Summary of any successful penetration scenarios
▪Detailed listing of all information gathered during penetration testing
▪Detailed listing of all vulnerabilities found
▪Description of all vulnerabilities found
▪Suggestions and techniques to resolve vulnerabilities found



2.3.8 SSL Weak Cipher Suites Supported

Ease of exploitation	Not so Easy	Threat impact rating	Medium
Port	TCP/ 443	OS type	Linux Kernel 2.6 on Ubuntu 8.04
Finding	The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.		
Affected resource	192.***.***.23		
Results	The remote service encrypts traffic using a protocol with known weaknesses; in which attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.		

POC

```
Testing SSL server 192.168.53.111 on port 443

 Supported Server Cipher(s):
   Accepted  SSLv3  256 bits  DHE-RSA-AES256-SHA
   Accepted  SSLv3  256 bits  AES256-SHA
   Accepted  SSLv3  128 bits  DHE-RSA-AES128-SHA
   Accepted  SSLv3  128 bits  AES128-SHA
   Accepted  SSLv3  168 bits  EDH-RSA-DES-CBC3-SHA
   Accepted  SSLv3  56 bits   EDH-RSA-DES-CBC-SHA
   Accepted  SSLv3  168 bits  DES-CBC3-SHA
   Accepted  SSLv3  56 bits   DES-CBC-SHA
   Accepted  SSLv3  128 bits  RC4-SHA
   Accepted  SSLv3  128 bits  RC4-MD5
   Accepted  TLSv1  256 bits  DHE-RSA-AES256-SHA
   Accepted  TLSv1  256 bits  AES256-SHA
   Accepted  TLSv1  128 bits  DHE-RSA-AES128-SHA
   Accepted  TLSv1  128 bits  AES128-SHA
   Accepted  TLSv1  168 bits  EDH-RSA-DES-CBC3-SHA
   Accepted  TLSv1  56 bits   EDH-RSA-DES-CBC-SHA
   Accepted  TLSv1  168 bits  DES-CBC3-SHA
   Accepted  TLSv1  56 bits   DES-CBC-SHA
   Accepted  TLSv1  128 bits  RC4-SHA
   Accepted  TLSv1  128 bits  RC4-MD5
```

Risk Mitigation

Reconfigure Apache to disable weak cipher support by using following instructions

1. Edit the httpd.conf or ssl.conf file to include the following line:
   SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2. Restart your Apache process by running the command below.
   # /etc/init.d/apache2 restart

Reference	http://www.openssl.org/docs/apps/ciphers.html

Tools and Methodologies

As professional security consultants, we only employ methodologies that are internationally recognised to ensure that every penetration testing activity is governed by acceptable rules and regulations:

- Guidelines
  - OSSTMM :The Open Source Security Testing Methodology Manual.
  - OWASP :Open Web Application Security Project.
- Tools
  - NMAP,Nikito,John,CAIN&Able and many more…………..
  - Whopix
  - Tigertools (Commercial Tool)
  - Metasploit.
  - ExploitTree.
  - Core Impact (Commercial Tool)

Partial List of What Hackers Can Do

- Whois Discovery
- MX records for email servers
- Nslookup and attempt zone transfers
- NMAP ping sweep and intense scanning
- Traceroute for hops vulnerabilities
- SMTP exploits : EHLO, send message for phishing etc
- Find vulnerabilities – Netcat, Nessus, Metasploit
- Exploit and attack: brute force, sniffers, password crackers etc
- Obtain banners, ascertain systems
- SNMP string exploits
- Install rootkits, trojans and malware
- Remove logs and clean up tracks
- War Driving
- Crack WEP (Wepcrack, airsnort etc)
- Web Page crawl and internet trawling
- Review SSL/TLS
- Identify Authentication methods, AD
- SQL injection
- Buffer overflow
- XSS
- Input limitation
- HTTP headers
- Hidden content, info leaks (robot.txt etc)
- Crack sessions
- Lockout mechanisms
- And Thousands more

Qualifications of Our Security Specialists

GIAC CERTIFIED PENETRATION TESTER
GPEN

GIAC REVERSE ENGINEERING MALWARE
GREM

GIAC SECURITY ESSENTIALS CERTIFIED
GSEC

GIAC CERTIFIED FORENSIC ANALYST
GCFA

GIAC CERTIFIED INCIDENT HANDLER
GCIH

PENETRATION
LICENSED
TESTER

C|EH™
Certified Ethical Hacker

C|HFI™
Computer Hacking Forensic INVESTIGATOR

CGEIT®
Certified in the Governance of Enterprise IT®
An ISACA® Certification

CISM®
Certified Information Security Manager®
An ISACA® Certification

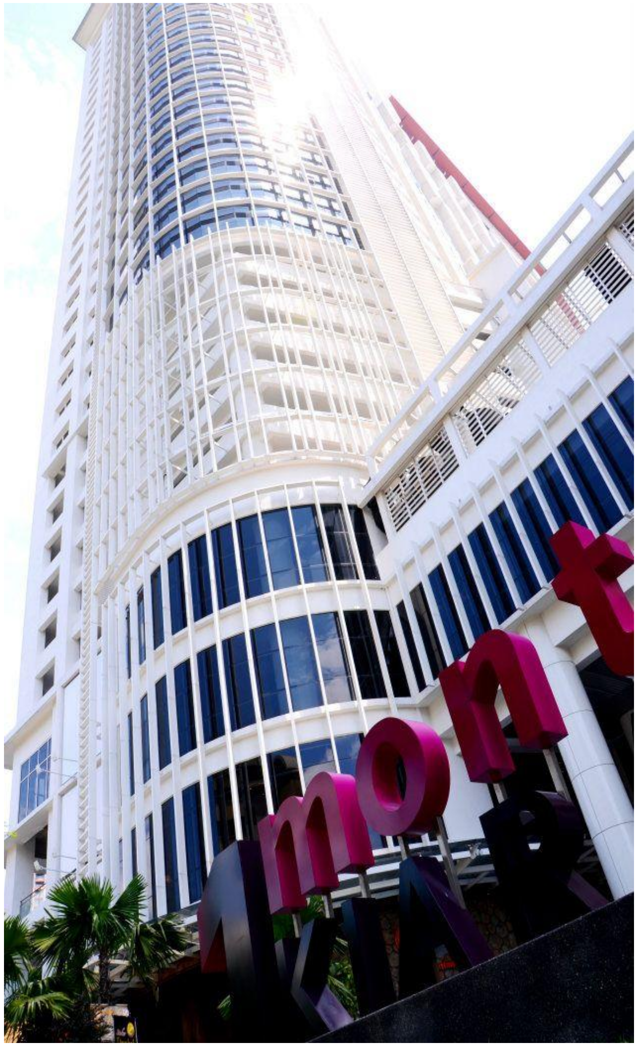
CISA®
Certified Information Systems Auditor®
An ISACA® Certification

FOR MORE INFORMATION

Will **YOU** become a target for hackers?

It is not a matter of **IF**, but **WHEN**.

Contact us for our Penetration Testing Services today!



PKF AvantEdge Penetration Testing Service

Email:	avantedge@pkfmalaysia.com
Web:	http://www.pkfmalaysia.com
Address:	Level 33, Menara 1MK, Kompleks 1 Mont' Kiara, No.1, Jalan Kiara, Mont' Kiara 50480 Kuala Lumpur
Telephone:	+6019 278 8629 (Mr Stevie Heong) +6016 213 2186 (Mr CB Chan)
Facsimile:	+603 6201 8880