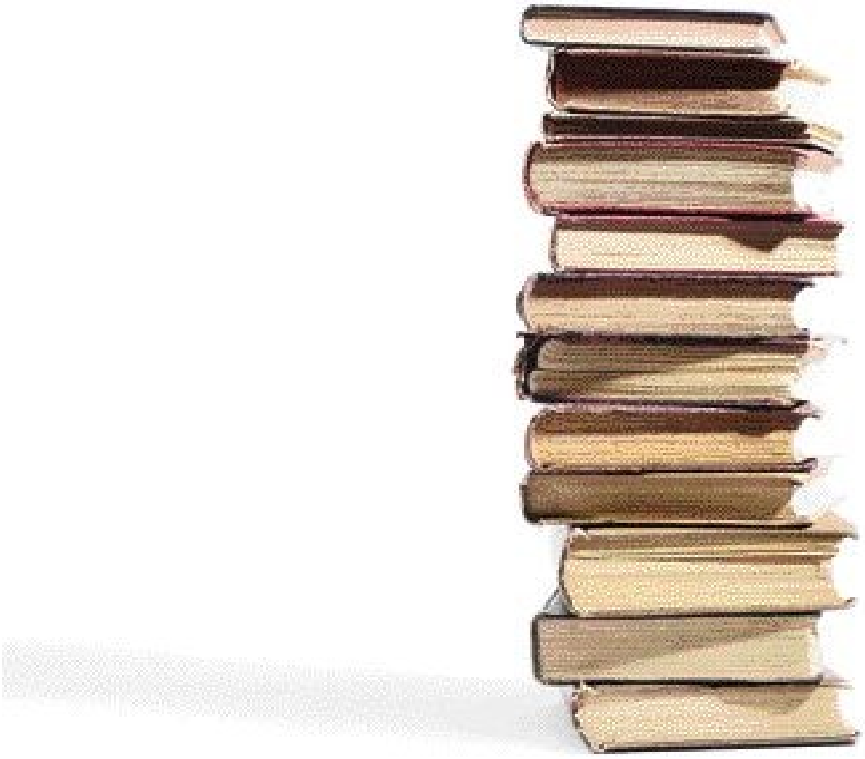


Penetration Testing | Hacking

sup3r
sup3r@usa.com

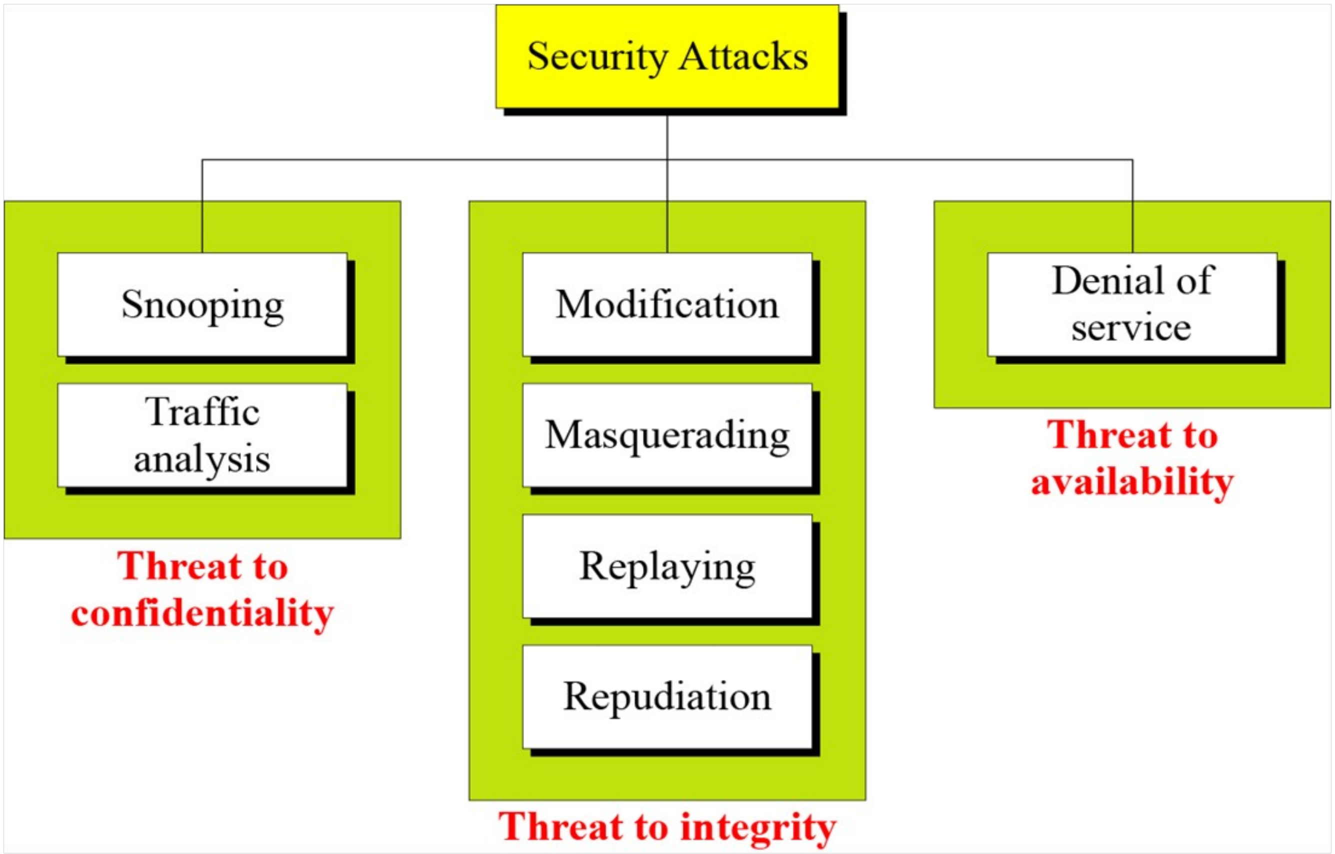
INTEGRITY
AVAILABILITY
CONFIDENTIALITY

CIA triad

Confidentiality
Keeping information secret from unauthorized access

Integrity
Changes should be done only by authorized users and through authorized mechanism

Availability
The information created and stored need to be available to authorized users and application



Threat to confidentiality

- snooping :

refers to unauthorized access to or interception of data

- Traffic analysis :

monitoring online traffic

Threat to integrity

1. Modification :

refers to type of attack in which the attacker modifies the information to make it beneficial to themselves

2.spoofing (Masquerading):

happen when the attackers impersonate somebody else .

3. Replaying:

th attacker obtain a copy of message sent by user and later tries to replay it

4. Repudiation:

happens when one of the tow parties in the communication deny sending or receiving message.

1. **Threat to availability**

1. Denial of service:

attacks may slow down or totally interrupt the service of the system
Causing the application to consume system resources excessively or to stop functioning altogether

Vulnerabilities

vulnerability is a weakness which allows an attacker to reduce a system's information Assurance.

- Weakness of an asset that can be exploited by a threat.

HACKERS

ScriptKiddie :

is a derogatory term used to describe those who use scripts or programs developed by others to attack computer systems and networks and deface websites

Lamerz:

Lamer is a jargon or slang name originally applied in cracker and phreaker culture to someone who didn't really understand what he or she was doing. Today it is also loosely applied by IRC, BBS, and online gaming users to anyone perceived to be contemptible. In general, the term has come to describe someone who is intentionally ignorant of how things work.

Black Hat:
A black hat is the villain or bad guy, especially in a western movie in which such a character would wear a black hat in contrast to the hero's white hat.

The phrase is often used figuratively, especially in computing slang, where it refers to a computer security hacker that breaks into networks or computers, or creates computer viruses

White Hat:
A white hat in computing slang refers to an *ethical hacker*, penetration tester, cracker or security consolidator.[1] White hat hackers are computer security experts, who specialize in penetration testing, and other testing methodologies, to ensure that a company's information systems are secure. White hat hackers are also called "sneakers"[2], red teams, or tiger teams[3]. These security experts may utilize a variety of methods to carry out their tests, including DoS attacks social engineering tactics, use of hacking tools, such as W3af, LOIC (Low Orbit Ion Cannon), Metasploit, which identify and exploits known vulnerabilities, and attempts to evade security to gain entry into secured areas.

Grey hat :
A grey hat, in the hacking community, refers to a skilled hacker whose activities fall somewhere between white and black hat hackers on a variety of spectrums. It may relate to whether they sometimes arguably act illegally, though in good will, or to how they disclose vulnerabilities. They usually do not hack for personal gain or have malicious intentions, but may be prepared to technically commit crimes during the course of their technological exploits in order to achieve better securit

Penetration Test :

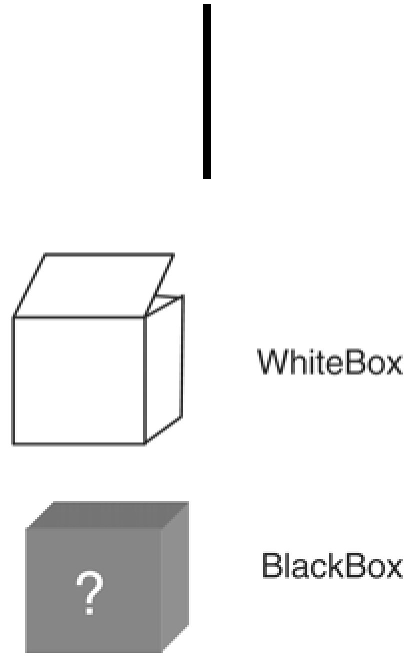
A penetration test, occasionally pentest, is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical counterme asuresnted to the system owner, together with an assessment of their impact, and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

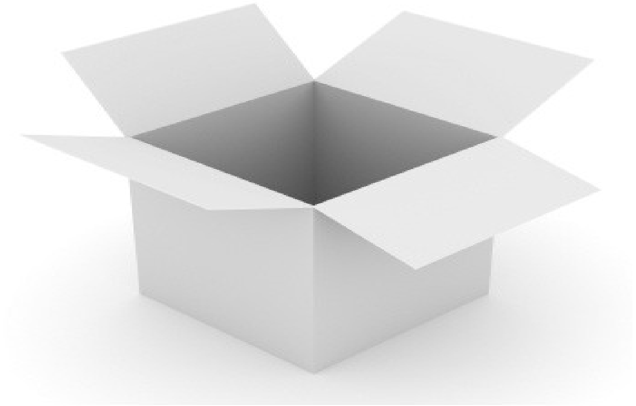
Penetration Test

Penetration test (white hat attacks)

Penetration testing (also called pen testing) is the practice of testing a computer system , network or web application to find vulnerabilities that an attacker could exploit.

Penetration Test





White-box testing (a.k.a. clear box testing, glass box testing, transparent box testing, or structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are required and used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT).

While white-box testing can be applied at the unit, integration and system levels of the software testing process, it is usually done at the unit level. It can test paths within a unit, paths between units during integration, and between subsystems during a system level test. Though this method of test design can uncover many errors or problems, it might not detect unimplemented parts of the specification or missing requirements.

White-box test design techniques include:

- Control flow testing
- Data flow testing
- Branch testing
- Path testing

Black-box testing is a method of software testing that tests the functionality of an application as opposed to its internal structures or workings (see white-box testing). Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. Test cases are built around specifications and requirements, i.e., what the application is supposed to do. It uses external descriptions of the software, including specifications, requirements, and design to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure.

This method of test can be applied to all levels of software testing: unit, integration, functional, system and acceptance. It typically comprises most if not all testing at higher levels, but can also dominate unit testing as well.

Brute Force attack :

a brute force attack is a strategy used to break the encryption of data . It involves traversing the search space of possible keys until the correct key is found

Dictionary Attack :

A type of password attack that does not attempt to decrypt any information but simply tries each of the words in a dictionary in hopes that the user has used one of the words as his or her password

Denial of Service:

a DoS attack is a from of attacking another computer or company by sending millions or more requests every second causing the network to slow down , cause errors or shut down

The Ten Most Critical Web Application Security Vulnerabilities

1- Cross Site Scripting

2- Injection Flows

3- Malicious File Execution

4- Insecure Direct Object Reference

5- Cross Site Scripting

6- Information Leakage

7- Session Management

8- Insecure Cryptographic Storage

9- Insecure Communication

10- Failure to Restrict URL Access

Cross Site Scripting

- Better known as XSS is in fact a subset of HTML injection
- XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content .
- XSS allows attackers to execute script in the victim's browser which can hijack user sesions, deface web sites , possibly introduce worms , etc
- the malicious script is usually JavaScript , but any scripting language supported by the victim's browser is a potential target for this attack .

Injection Flaws

Injection flaws, particularly SQL injection , are common in web application injection occurs when user-supplied data is sent to an interpreter as part of a command or query, The attacker's hostile data tricks the interpreter into executing unintended commands or changing data .

Malicious File Execution

Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks , such as total server compromise .
Malicious file execution attacks affect PHP,XML and any framework which accepts filenames or files from users.

Insecure Direct Object Reference

A direct object reference occurs when a developer exposes a reference to an internal implementation object , such as a file, directory, database record, or key, as a URL or from parameter. Attackers can manipulate those references to access other object without authorization

Cross Site Scripting

A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to v vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks

information leakage and Improper Error Handling

Application can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems.
Attackers use this weakness to steal sensitive data, or conduct more serious attacks.

Broken Authentication and Session Management

Account credentials and session tokens are often not properly protected.
Attackers compromise passwords, keys, or authentication tokens to assume other users' identities

Insecure Cryptographic Storage:

Web application rarely use cryptographic functions properly to protect data and credentials, attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud

Insecure Communication

application frequently fail to encrypt network traffic when it is necessary protect sensitive communications

Failure to Restrict URL Access

Frequently,an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users, Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly

thanks

by sup3r