***

STEPS followed by White Hat Hackers

1> Legal documentation LSI VPG PRP R

2> Scope assessment

3> Information assessment

4> Vulnerability assessment

5> Penetration testing

6> Gaining access

7> Privilage escalation

8> Report generation

9> Patch assistance

10> Revalidation

Legal documentation :

- NDA (Non disclosure agreement)
- MOU (Memorandum of understanding)

<u>NDA</u>: A contract by which both the Parties agree not to disclose confidential information that they have shared with each other.

-> Testing activity

-> Bugs found

-> Any confidential information

MOU: It is the ~~devices~~ document that regulates the act of Security expert.

-> Devices | Network to be tested
-> Upto which extent it has to be tested.

Finicial Agreement: How much money has to be Paid for the testing.

2) Scope Assessment:

It is the document that regulates the act of security expert which Prevents him from accessing unauthorized devices | networks.

-> At what extent security testing has to be carried out.
-> What are the devices has to be tested
-> What are the networks that has to be tested for security.

3) Information Gathering:

The Phase where the compay Provides some basic information about network | devices that has to be tested & information is assessed by security expert to carry out his future testing activity.

- Types of OS used
- Programming Language used
- Architecture of website | application
- Test Account details | Admin access

4) Vulnerability Assesment

A vulnerability assesment is the Process of identifying, quantifying & Priortizing the vulnerabilities in a system.

5) Penetration Testing :

a The Pen Testing is a security exercise where a cyber-security expert attempts to find exploit vulnerabilities in a computer system

6) Gaining Access

This Phase is where an attacker breaks into system | network using various tools or techniques.

7) Privilage escalation:

The Process of transforming from a normal user to admin.

8) Report generation: & how it is Presenti

The final report, is the most important step of security testing.

-> A good security tester should be able to clearly Present his findings to non tech executiv & System admistrators.

Extreme
13-15
High
10-12
elevated
7-9
Moderate
4-6
Low
1-3

9) Patch assistance:

- once the vulnerbilities are found out, it has to be Patched to improve security.
- Then security expert then Provides SUPPort for developers & helps them in Patching bugs.

10) Revalidation

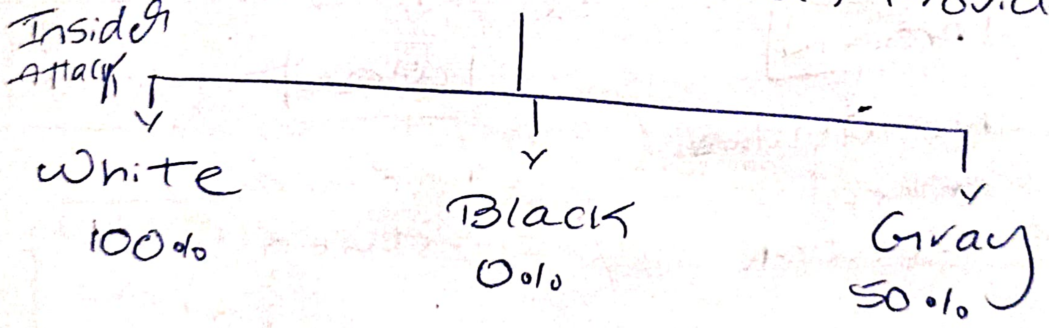
-> After Patching the bugs the security expert has to find out if the bugs have been completely Patched or not.

-> If not Patched, the security expert has to assist developers again.

Types of security Testing :

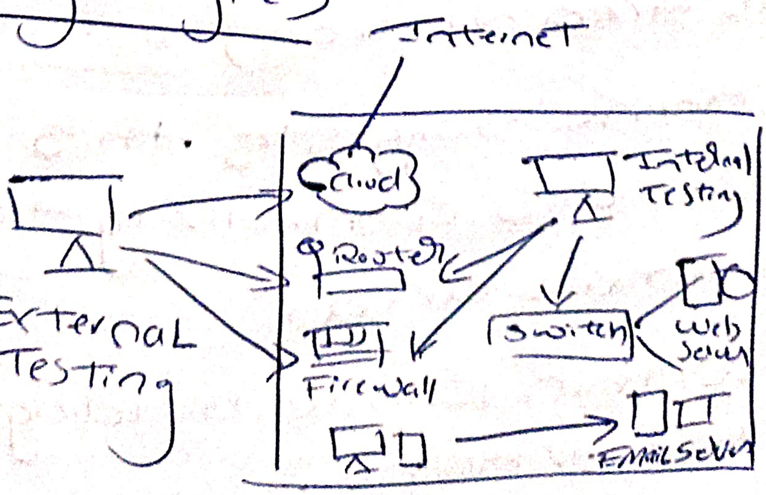
security testing is carried by white hat hacker or security experts also called as Pen Testing.

Based on Information Provided



Testing 2Types

Based on Location of Testing



External
Internal.