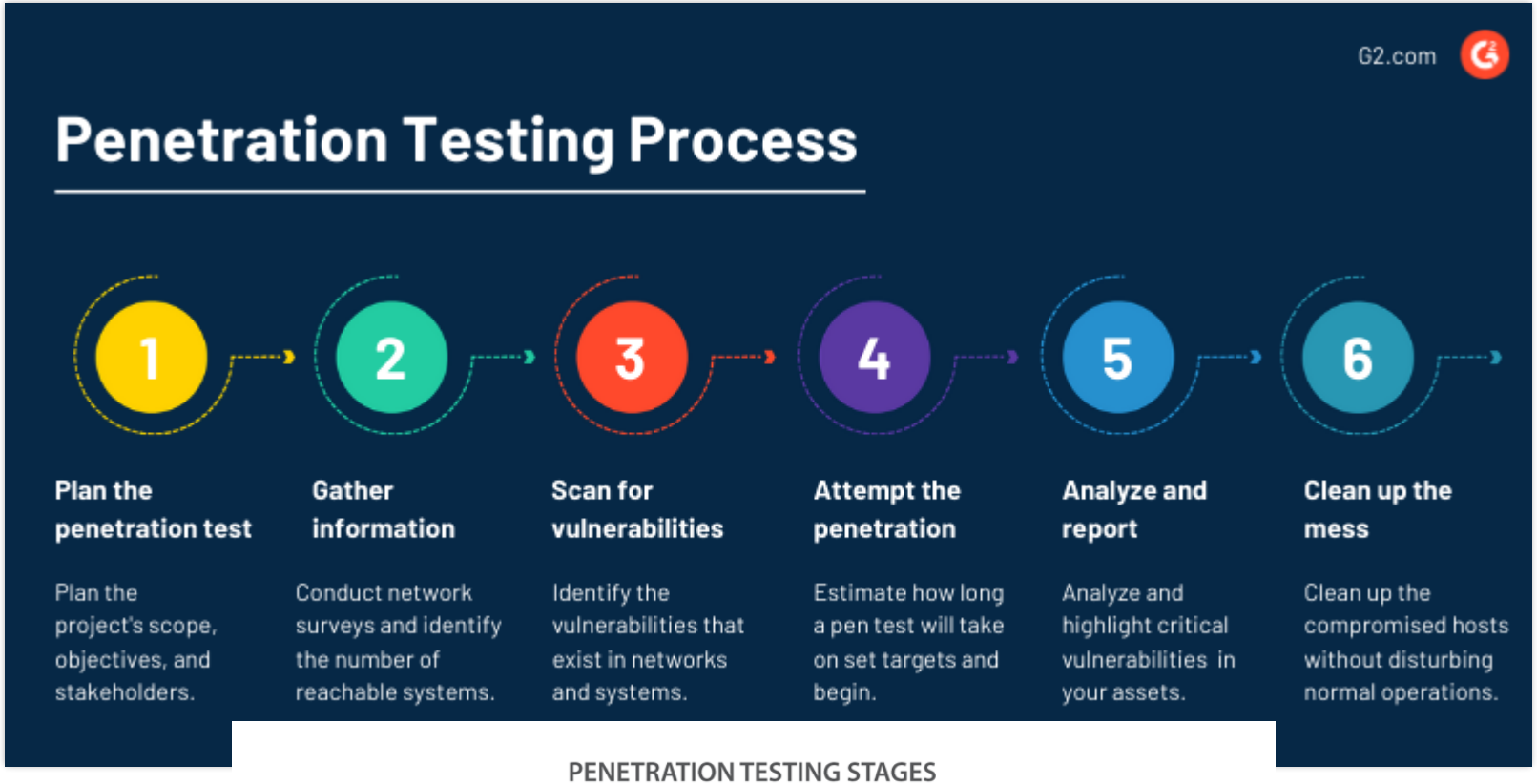
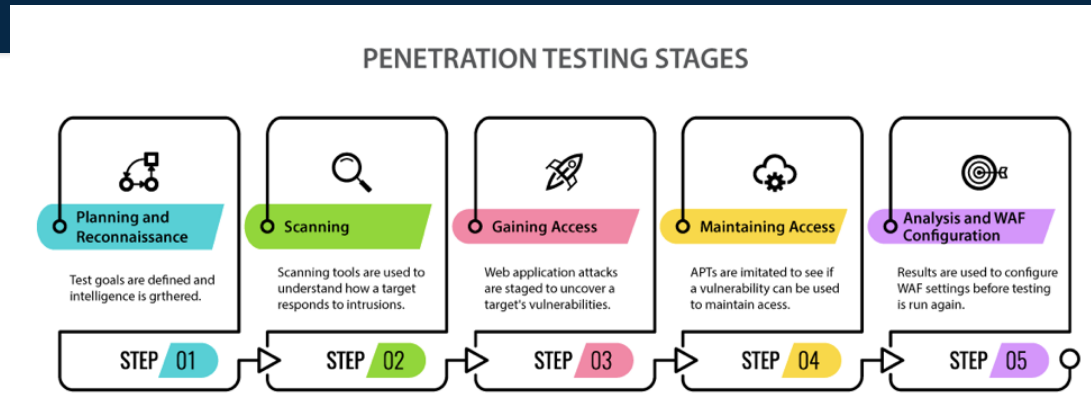
Phases of Penetration Testing

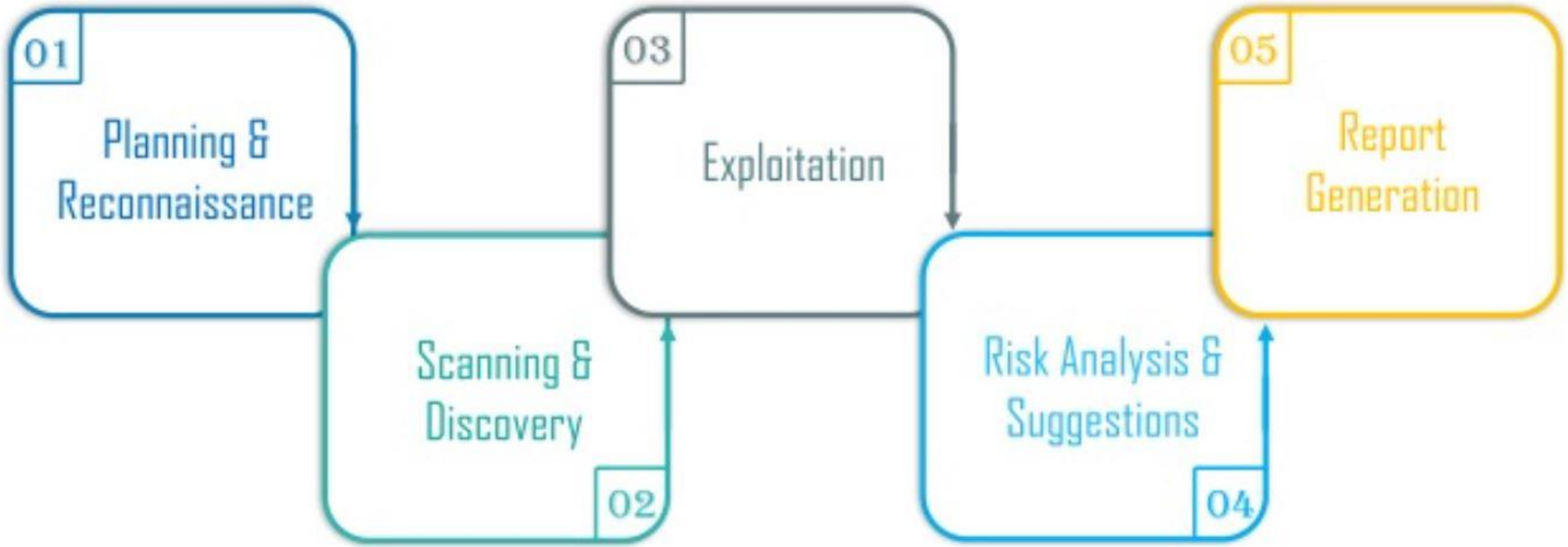
Dr. Zahid Hussain Qaisar


G2.com
Penetration Testing Process
1
2
3
4
5
6
Plan the penetration test
Plan the project's scope, objectives, and stakeholders.
Gather information
Conduct network surveys and identify the number of reachable systems.
Scan for vulnerabilities
Identify the vulnerabilities that exist in networks and systems.
Attempt the penetration
Estimate how long a pen test will take on set targets and begin.
Analyze and report
Analyze and highlight critical vulnerabilities in your assets.
Clean up the mess
Clean up the compromised hosts without disturbing normal operations.


PENETRATION TESTING STAGES
Planning and Reconnaissance
Test goals are defined and intelligence is grthered.
STEP 01
Scanning
Scanning tools are used to understand how a target responds to intrusions.
STEP 02
Gaining Access
Web application attacks are staged to uncover a target's vulnerabilities.
STEP 03
Maintaining Access
APTs are imitated to see if a vulnerability can be used to maintain acess.
STEP 04
Analysis and WAF Configuration
Results are used to configure WAF settings before testing is run again.
STEP 05


PENETRATION TESTING PROCESS
RECONNAISSANCE
Gather as much information about a target using active or passive means.
SCANNING
Scan the target host for Vulnerabilities. Perform port scan, network scan, and vulnerability scan.
GAINING ACCESS
Exploit Vulnerabilities and gain access to target host
MAINTAINING ACCESS
Maintain access to the system using backdoors or by other means
CLEARING TRACKS
Delete logs and stuff that were used during the process to avoid tracing and detection
REPORTING
Report the Vulnerabilities identified during the process along with exploit details, impact and remediation.
https://hacksheets.in

Penetration Testing Phases



- **What are the phases of a penetration test?**
- Penetration tester usually begins by gathering as much information about the target as possible. Then he identifies the possible vulnerabilities in the system by scanning. After which he launches an attack. Post-attack he analyses each vulnerability and the risk involved. Finally, a detailed report is submitted to higher authorities summarizing the results of the penetration test.
- Penetration testing can be broken down into multiple phases, this will vary depending on the organization and the type of penetration test.
- Let's discuss each phase:
- **Reconnaissance & Planning**
- The first phase is planning. Here, the attacker gathers as much information about the target as possible. The data can be IP addresses, domain details, mail servers, network topology, etc. In this phase, he also defines the scope and goals of a test, including the systems to be addressed and the testing methods to be used. An expert penetration tester will spend most of the time in this phase, this will help with further phases of the attack.

- **Scanning**
- Based on the data collected in the first step, the attacker will interact with the target with an aim to identify the vulnerabilities. This helps a penetration tester to launch attacks using vulnerabilities in the system. This phase includes the use of tools such as port scanners, ping tools, vulnerability scanners, and network mappers.
- While testing web applications, the scanning part can be either dynamic or static.
- In static scanning, the aim is to identify the vulnerable functions, libraries, and logic implementation
- Dynamic analysis is the more practical way of scanning compared to static analysis where the tester will pass various inputs to the application and record the responses
- **Actual Exploit**
- This is the crucial phase that has to be performed with due care. This is the step where the actual damage is done. Penetration Tester need to have some special skills and techniques to launch an attack on the target system. Using these techniques an attacker will try to get the data, compromise the system, launch dos attacks, etc. to check to what extent the computer system or application or a network can be compromised.

- After the penetration test is complete, the final goal is to collect the evidence of the exploited vulnerabilities. This step mostly considers all the steps discussed above and an evaluation of the vulnerabilities present in the form of potential risks. Sometimes, in this step pen-tester also provides some useful recommendations to implement in order to improve security levels.
- **Report Generation**
- Now, this is the final and the most important step. In this step, the results of the penetration test are compiled into a detailed report. This report usually has the following details:

- Recommendations made in the previous phase
- Vulnerabilities that were discovered and the risk levels they posses
- Overall summary of the penetration test
- Suggestions for future security

- Pentesting begins with the *pre-engagement* phase, which involves talking to the client about their goals for the pentest, mapping out the scope (the extent and parameters of the test), and so on. When the pentester and the client agree about scope, reporting format, and other topics, the actual testing begins.
- In the *information-gathering* phase, the pentester searches for publicly available information about the client and identifies potential ways to connect to its systems.
- In the *threat-modeling* phase, the tester uses this information to determine the value of each finding and the impact to the client if the finding permitted an attacker to break into a system. This evaluation allows the pentester to develop an action plan and methods of attack. Before the pentester can start attacking systems, he or she performs a
- *vulnerability analysis*. In this phase, the pentester attempts to discover vulnerabilities in the systems that can be taken advantage of in the *exploitation* phase. A successful exploit might lead to a *post-exploitation* phase, where the result of the exploitation is leveraged to find additional information, sensitive data, access to other systems, and so on.
- Finally, in the *reporting* phase, the pentester summarizes the findings for both executives and technical practitioners.

Thank you