Frameworks

Pre-Engagement:

This is the planning stage. Here, we decide what we're testing and how we're going to do it. It's like drawing a roadmap before a trip.

Reconnaissance:

This is the research phase. We gather all the information we can find about the target, just like you would look up a place before visiting it.

Enumeration/Scanning:

Now, we're trying to figure out what software and services the target system is using, kind of like identifying the locks on a door. This is where we use tools like nmap, which is like a digital keyring.

Exploitation:

At this point, we take advantage of the weak spots we've found. It's like using a key from our keyring (found during the scanning phase) to open a lock.

Privilege Escalation:

Once we're in, we try to get more access. This can be either moving sideways (accessing other accounts with the same level of access) or moving upwards (getting admin-level access). Think of it as getting into a building and then trying to find a way into other rooms or floors.

Post-Exploitation:

This stage has a few parts:

- Full Privilege Collection: As a high-level user, we collect more sensitive data. It's like finding the boss's office and looking through their files.
- Pivoting: We look for other potential targets. Like seeing if the boss's office has a door to other parts of the building.
- Clean-Up: We erase evidence of our presence, similar to wiping our fingerprints off everything we've touched.
- Reporting: We document everything we did: what we found, how we found it, the tools and commands we used, etc. This is like writing a detailed trip report after a journey.

Remediation:

Finally, we fix the problems we found and suggest ways to prevent them in the future. This is like fixing the locks we managed to open and recommending better security measures.

Framework	Description	Why They Differ
OSSTMM	A guidebook for testing operational security of physical locations, workflow, human security, physical security, wireless security, telecommunication security, data networks security, and compliance.	OSSTMM focuses on operational security and covers a wide range of security aspects, making it suitable for assessing the overall security of an organization.
NIST 800-115	A free-to-use document that includes templates, techniques, and tools for assessing many types of systems and scenarios. It's not as detailed as ISSAF or OSSTMM, but provides a repeatable process for conducting security reviews .	NIST 800-115 provides a standardized approach to security reviews and is widely recognized and accepted in the industry. It focuses on providing a solid foundation for an organization's security posture.

PTES	A methodology developed to cover the key parts of a penetration test, from the initial contact phase, working through the stages of the cyber kill chain (e.g. vulnerability analysis, exploitation, and post-exploitation) and finishing with the reporting phase	**PTES** focuses specifically on penetration testing and follows a systematic approach, covering all the key phases of a penetration test. It provides a detailed technical guide for testers.
OWASP	A framework with a strong focus on web application security throughout the entire software development lifecycle. It's not limited to Web Applications alone, depending on the type of application, the testing guide is further broken down into three; OWASP Web Security Testing Guide (WSTG), OWASP Mobile Security Testing Guide (MSTG), OWASP Firmware Security Testing Methodology	**OWASP** Focuses on web application security, provides guides for different types of applications
Web Application	**Not a framework**, but a type of application that is tested using frameworks like OWASP.	
Firmware	**Not a framework,** but a type of software that provides low-level control for a device's	

	specific hardware. It can be tested using methodologies like the OWASP Firmware Security Testing Methodology.	
Mobile Security	**Not a framework**, but a field of security that focuses on securing mobile devices like smartphones and tablets.	
Penetration Testing Framework 0.59	A comprehensive hands-on penetration testing guide that lists usage of the testing tools in each testing category 1.	**PTF** Provides a comprehensive guide for penetration testing, includes a list of tools for each testing category
ISSAF	A very good reference source of penetration testing that provides comprehensive penetration testing technical guidance. It's not an active community but is a complex, structured, and specialized penetration testing methodology	**ISSAF** Provides a comprehensive guide for penetration testing, includes recommendations on tools to use in each step