Penetration Testing Introduction: Log4Shell(CVE-2021-44228)

Pre-Engagement:

Pre-engagement in the context of Log4shell would have included learning about Apache Log4j, how it is used in the intended environment, and any known vulnerabilities. Using this data, a plan for checking the target environment for Log4shell vulnerabilities would have been created.

Intelligence Gathering:

Information about exploit code, target systems, and known Log4shell vulnerabilities would have been gathered as part of the intelligence gathering process in the case of Log4shell. This data would have been utilized to create mitigation plans and evaluate the danger of Log4shell attacks.

Threat Modeling:

Threat modeling in the context of Log4shell would have entailed locating possible adversaries who might take advantage of Log4shell vulnerabilities. These risks could be the unauthorized access to private information, the runtime of arbitrary programs, or the interruption of vital services.

Vulnerability Analysis:

Vulnerability analysis in the context of Log4shell would have involved determining which systems within the target environment were susceptible to Log4shell. This would have required manually checking the code for potential vulnerabilities and scanning the target environment for Log4shell vulnerabilities.

Exploitation:

An attacker must figure out how to insert malicious code into a Log4j log message in order to take advantage of Log4shell.

This can be done in a number of ways, such as:

- Sending a specially crafted HTTP request to a vulnerable application.
- Uploading a malicious file to a vulnerable application.
- Exploiting another vulnerability in a vulnerable application to gain access to a log file.

When a Log4j log message is processed, the malicious code that has been injected into it will be run. The attacker may then have total control over the weak system as a result.

Reporting: At this step, the penetration tester or team will provide a written document on their discoveries and provide risk analysis on the discoveries.