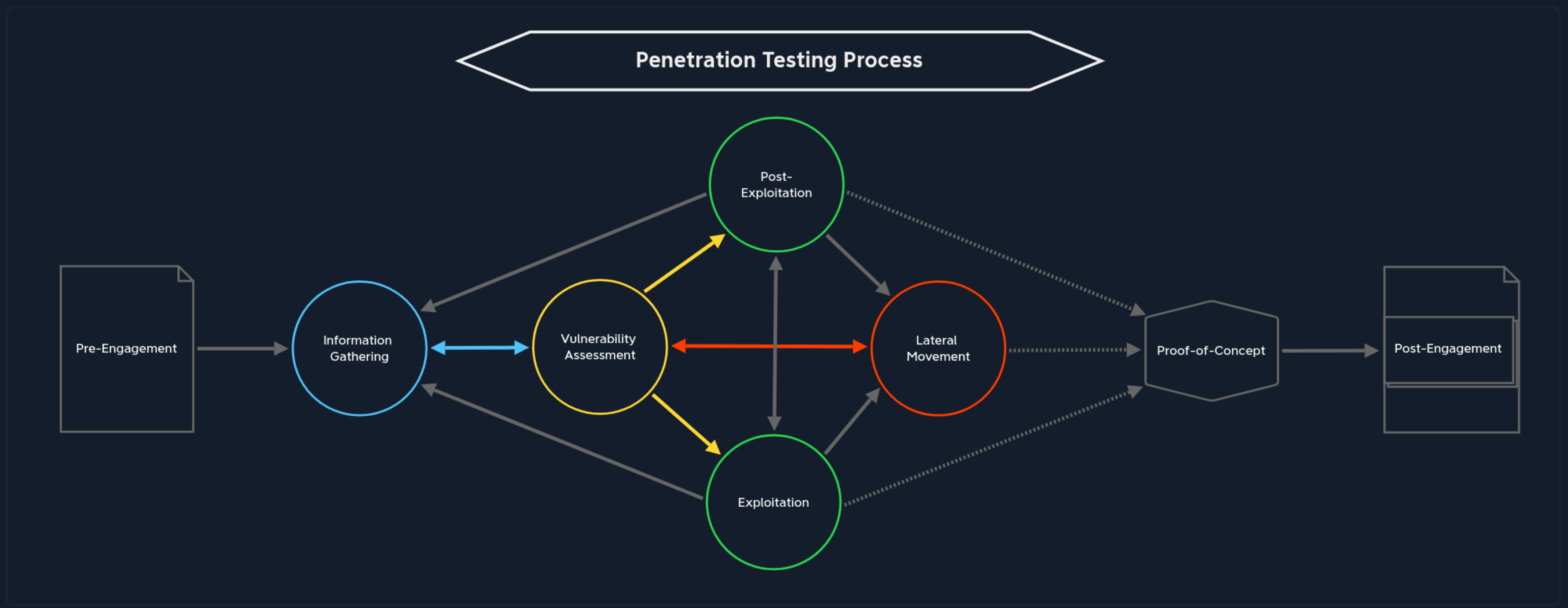
Vulnerability Assessment

During the `vulnerability assessment` phase, we examine and analyze the information gathered during the information gathering phase. The vulnerability assessment phase is an analytical process based on the findings.



`An analysis is a detailed examination of an event or process, describing its origin and impact, that with the help of certain precautions and actions, can be triggered to support or prevent future occurrences.`

Any analysis can be very complicated, as many different factors and their interdependencies play a significant role. Apart from the fact that we work with the three different times (past, present, and future) during each analysis, the origin and destination play a significant role. There are four different types of analysis:

Analysis Type	Description
`Descriptive`	Descriptive analysis is essential in any data analysis. On the one hand, it describes a data set based on individual characteristics. It helps to detect possible errors in data collection or outliers in the data set.
`Diagnostic`	Diagnostic analysis clarifies conditions' causes, effects, and interactions. Doing so provides insights that are obtained through correlations and interpretation. We must take a backward-looking view, similar to descriptive analysis, with the subtle difference that we try to find reasons for events and developments.
`Predictive`	By evaluating historical and current data, predictive analysis creates a predictive model for future probabilities. Based on the results of descriptive and diagnostic analyses, this method of data analysis makes it possible to identify trends, detect deviations from expected values at an early stage, and predict future occurrences as accurately as possible.
`Prescriptive`	Prescriptive analytics aims to narrow down what actions to take to eliminate or prevent a future problem or trigger a specific activity or process.

We use our results and information obtained so far and analyze them to make conclusions. The formation of conclusions can be extended very far, but we must then confirm or disprove them. Suppose we found an open TCP port 2121 on a host during the information-gathering phase.

Other than the fact that this port is open, Nmap did not show us anything else. We must now ask ourselves what conclusions can be drawn from this result. Therefore, it does not matter which question we start with to make our conclusions. However, it is essential to ask `precise questions` and remember what we `know` and `do not know`. At this point, we must first ask ourselves what we `see` and what we actually `have`, because what we see is not the same as what we have:

- a `TCP` port `2121`. - `TCP` already means that this service is `connection-oriented`.
- Is this a `standard` port? - `No`, because these are between `0-1023`, aka well-known or system ports
- Are there any numbers in this `port number` that look `familiar`? - `Yes`, `TCP` port `21` (`FTP`). From our experience, we will get to know many standard ports and their services, which administrators often try to disguise, but often use "easy to remember" alternatives.

Based on our guess, we can try to connect to the service using `Netcat` or an `FTP` client and try to establish a connection to confirm or disprove our guess.

While connecting to the service, we noticed that the connection took longer than usual (about 15 seconds). There are some services whose connection speed, or response time, can be configured. Now that we know that an FTP server is running on this port, we can deduce the origin of our "failed" scan. We could confirm this again by specifying the minimum `probe round trip time` (`--min-rtt-timeout`) in Nmap to 15 or 20 seconds and rerunning the scan.

Vulnerability Research and Analysis

`Information Gathering` and `Vulnerability Research` can be considered a part of descriptive analysis. This is where we identify the individual network or system components we are investigating. In `Vulnerability Research`, we look for known vulnerabilities, exploits, and security holes that have already been discovered and reported. Therefore, if we have identified a version of a service or application through information gathering and found a Common Vulnerabilities and Exposures (CVE), it is very likely that this vulnerability is still present.

We can find vulnerability disclosures for each component using many different sources. These include, but are not limited to:

CVEdetails	Exploit DB	SecurityFocus
Packet Storm Security	NIST	Vulners

This is where `Diagnostic Analysis` and `Predictive Analysis` is used. Once we have found a published vulnerability like this, we can diagnose it to determine what is causing or has caused the vulnerability. Here, we must understand the functionality of the `Proof-Of-Concept` (`POC`) code or the application or service itself as best as possible, as many manual configurations by administrators will require some customization for the POC. Each POC is tailored to a specific case that we will also need to adapt to ours in most cases.

Assessment of Possible Attack Vectors

`Vulnerability Assessment` also includes the actual testing, which is part of `Predictive Analysis`. In doing so, we analyze historical information and combine it with the current information that we have been able to find out. Whether we have received specific evasion level requirements from our client, we test the services and applications found `locally` or `on the target system`. If we have to test covertly and avoid alerts, we should mirror the target system locally as precisely as possible. This means we use the information obtained during our information gathering phase to replicate the target system and then look for vulnerabilities in the locally deployed system.

The Return

Suppose we are unable to detect or identify potential vulnerabilities from our analysis. In that case, we will return to the `Information Gathering` stage and look for more in-depth information than we have gathered so far. It is important to note that these two stages (`Information Gathering` and `Vulnerability Assessment`) often overlap, resulting in regular back and forth movement between them. We will see this in many videos where the author is solving an HTB box or some CTF challenge. We should remember that these challenges are often solved as fast as possible, and therefore speed is more important than quality. In a CTF, the goal is to get on the target machine and `capture the flags` with the highest privileges as fast as possible instead of exposing all potential weaknesses in the system.

`A (real) Penetration Test is not a CTF.`

Here the `quality` and `intensity` of our penetration test and its analysis have the highest priority because nothing is worse if our client gets successfully hacked via a relatively simple vector that we should have uncovered during our penetration test.

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 2 What type of analysis can be used to predict future probabilities?

Submit your answer here...

Submit

Previous Next

Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left