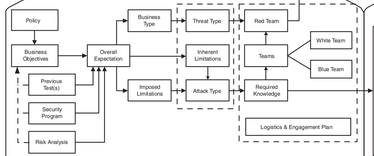
PLAN



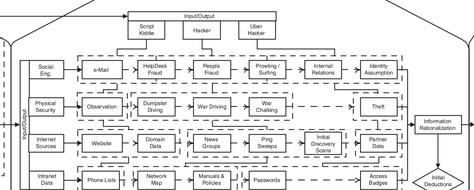
Starts with a Policy: Fully understanding the security policy of an organization is critical to the interpreted value of any security project.

Collect and Define: Leverage existing information security related data, combine with overall business objectives and establish expected outcome of test.

Threats and Limitations: Evaluate known threats, tactics and structure and compare to existing information and expectations to devise an attack type, profile of required knowledge, and imposed limitations

Management: Create teams, provide operational and communication protocols, and create metrics to ensure clear measurement of success or failure factors

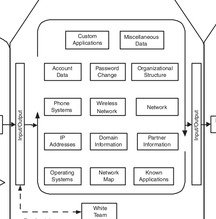
RECONNAISSANCE



Learn and Use: Based on the level and scope of required knowledge, the creation of an information and proposed collection tactic matrix should be used to acquire information about the target. Intensity and scope are defined by the business objectives and threat type, which in turn will establish the role collected data plays in the remainder of the engagement

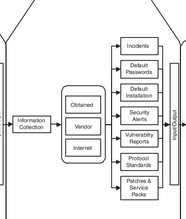
Rationalize: Depending on the tactic, depth, provided data, timeframe, and overall vulnerability of the target or the amount of freely available information, all data can be normalized and compared to seek other opportunities to gain information prior to moving into the next phase

ENUMERATE



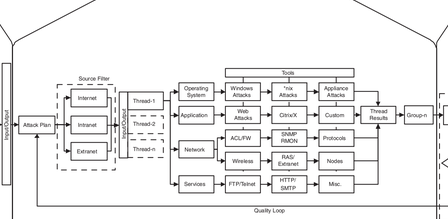
Direct Technical Investigation: By using various tools and specific information collected from the previous phase, systems, networks, services, and applications can be queried to gather empirical data on characteristics that can be used for an attack vector

ANALYSIS



Vulnerability Analysis: Data from the Internet, product vendors and even the target are reviewed for any documented alignment to a vulnerability

ATTACK

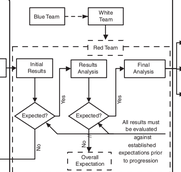


Attack Strategy: Based on the information learned about the target, overall objectives, expectations, limitations, and restrictions an attack plan can be formulated. The data will promote the use of one source point over another, or any combination of the three primary types

Quality Loop: Without a review of the initial thread results there is a greater possibility to loosing valuable vulnerability information or affecting the value of the test based on poor validation of a vulnerability thread

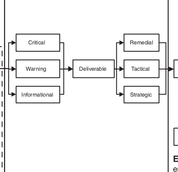
Groups of Threads: Threads represent a singularity of attack that can be combined to represent the total impact of a collection of threads or vulnerability. Multiple groups represent a web of vulnerabilities founded on technical as well as management vulnerabilities

RESULTS



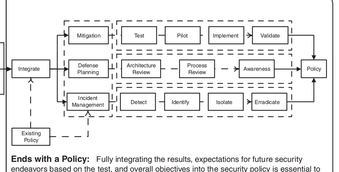
Always Compare and Review: Review Thread and Group data and combine to formulate other attack scenarios if time permits. Additionally, evaluate results against expectations and agreed upon tactics. If group results analysis continue to not meet expectations, you need to review the expectations of the test otherwise you will not be prepared for the results

DELIVERABLE



Risk is Key: The only method for ensuring a usable engagement document is to align with existing security policy, understanding of risk, and overall expectations (i.e. comparison of value of test to the value of data). Define a interpretation table and prioritize based on business demands, risk, and time

INTEGRATE



Ends with a Policy: Fully integrating the results, expectations for future security endeavors based on the test, and overall objectives into the security policy is essential to for value realization and better ROI on future test

Fix What is Broke: Based on the test's prioritized results, the first order of business is to address the remedial, risk reducing elements

Setup for Long-term ROI: Develop a clear operational and management structure to support full integration of security recommendations, establish an Information Security Management Program, and prepare for the next test

Response: Developing an incident response plan will be one of the few investments that get better with time. Create, evaluate, and test a response plan, document results and expectations, and prepare for the real thing