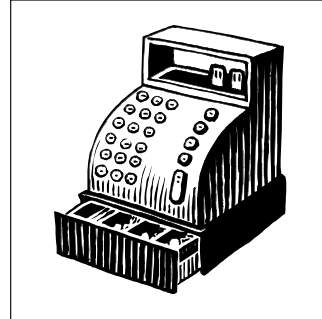


# 3 The Framework



What is a framework? Moreover, how does it apply to attacking a system? Finally, is a framework a methodology? A framework is collection of measurable tasks, whereas a methodology is a specific set of inputs, processes, and their outputs. A framework provides a hierarchy of steps, taking into consideration the relationships that can be formed when executing a task given a specific method.

For example, this book presents a framework of steps with options within each and they appear as chapters, headings, and so forth. The context within each section of this book introduces methods for performing certain tasks heeding the value represented by other points within the framework. When combined, an entire process geared towards value can be presented.

By formatting ethical hacking in a framework, as opposed to simply a collection of methods and tactics, elements can be easily removed and added to accommodate specific requirements of the test. Of course, the removal of a particular element within the framework can have repercussions when the goal of the entire framework is value.

How this applies to penetration testing is in ensuring the value of the test is realized. Given that a penetration test is part of a larger security program, one must include other characteristics of security to align the test appropriately to the demands driving it. Moreover, a framework highlights each phase, drawing relationships between them to make sure you're on track with the objectives. In addition, each step in the phase helps you take into account the nuances of performing a controlled attack. For example, there are limitations, inherent and imposed, that will have effects on each phase translating into varying degrees of value. Finally, it provides operational structure to the test. Knowing how and when to perform a task is as important as the task itself.

The mission of the framework is to explain the steps, their relation to other points within the performance of a test, and to expose the impact on value when excluding various methods within each. In the simplified Figure 3.1, we see each primary phase of the framework with points within each representing a task or value element. Some circles are larger than others, signifying more potential value. Depending on what tasks are not employed, some downstream elements may not be available simply because the required information or results from previous elements do not exist. Given that the framework is founded on related processes that span phases, the use (or omission) of a process will limit the availability or effectiveness of other processes.

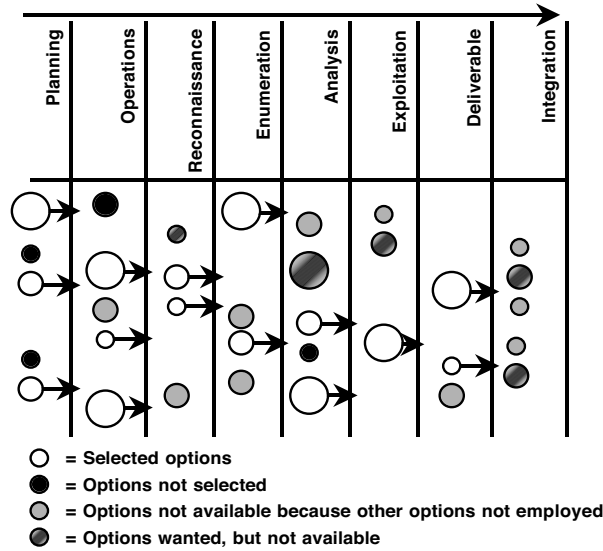


FIGURE 3.1 Determining the Impact on Value Based on Selected Options

Of course, for your specific goals of the test, the unselected or unavailable elements may prove to be of little or no value and therefore the impact is nonexistent. The important fact to evaluate is which elements are needed to meet your goals and understand there may be an inherent relationship to another point within the framework you have not considered or do not want to be exercised. The ability to gain visibility into the affiliation between one phase and another is the value a framework brings to the entire process.

While in its infancy, ethical hacking meant simply attacking a network and exploiting any vulnerability presenting itself; that was the goal—get in. And, quite frankly, this is still the M.O. for many engagements today. The tools have changed, the techniques are much more sophisticated, the knowledge of the consumers is much more comprehensive, but the essence of the test has remained much the same. Technique and tools are important and provide a strong foundation for further evolution, but with regard to security, the environment is too dynamic to base success on technique and tools alone. Racquetball is one of those sports of technique and tools: insightful volleys and a good racquet will win the match. However, the court does not change in size, the lines don't move, the back wall will always be there, and the environment is predictable.

With the absence of continuity, value rests on the shoulders of the tester and the framework that is followed. The ability to assess the situation and make quick determinations based on similar experiences is an attribute of a successful attack by today's standards.

On the other side of the equation is the recipient of these tests attempting to make value decisions based on his impression of a planned attack, an impression fed by security consultants, magazines, friends, and employees and not from extensive experience in being the target of hundreds of tests. I liken it to asking a regular



person to purchase food for a restaurant. They know what food is and have an understanding of value and use, but buying 250 pounds of meat, 10 gallons of mayonnaise, 25 pounds of cheese, and 8 boxes of detergent would challenge anyone not familiar with the process.

After performing and being involved with many penetration-testing engagements, there is a theme that begins to surface. People are not fully aware of the options available to them and how to apply those options to their environment. Many characteristics have varying degrees of intensity and requirements, such as information and limitations, that will influence other areas of the test and how they relate to the value of the test in an overall security program.

### PLANNING THE TEST

As with anything worth doing, proper planning is essential to performing a successful project. Planning provides an opportunity to evaluate existing business demands and processes, how they relate to a new business endeavor, and to make choices on which characteristics are worth doing and those in which you're not willing to accept risk.

Existing security policies, culture, laws and regulations, best practices, and industry requirements will drive many of the inputs needed to make decisions on the scope and scale of a test. Arguably, the planning phase of a penetration test will have a profound influence on how the test is performed and the information shared and collected, and will directly influence the deliverable and integration of the results into the security program.

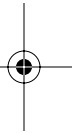
Planning describes many of the details and their role in formulating a controlled attack. Security policies, program, posture, and ultimately risk all play a part in guiding the outcome of a test. What drives a company's focus on security, its core business needs, challenges, and expectations will set the stage for the entire engagement.

### SOUND OPERATIONS

How is the test going to be supported and controlled? What are the underlying actions that must be performed regardless of the scope of the test? Who does what, when, where, how long, who is out of bounds, and what is in bounds of a test all need to be addressed. Logistics of the test will drive how information is shared and to what degree (or depth) each characteristic will be performed to achieve the desired results. Operational features will include determining what the imposed limitations of the tester are and how they are evaluated during the test.

### RECONNAISSANCE

Reconnaissance is the search for freely available information to assist in the attack. The search can be quick ping sweeps to see what IP addresses on a network will respond, scouring newsgroups on the Internet in search of misguided employees divulging useful information, or rummaging through the trash to find receipts for telecommunication services.





Reconnaissance can include theft, lying to people, tapping phones and networks, impersonations, or even leveraging falsified friendships to collect data about a target. The search for information is only limited by the extremes to which a customer and tester are willing to go.

The reconnaissance phase introduces many of the questions surrounding what actions truly provide value to the company. In this section, we examine the reconnaissance techniques, such as social engineering, and the necessary environmental characteristics that must exist to realize value from intense investigation. It is also in this section that the value of a certain type of test is questioned, which exposes the effects of poor planning or a poor understanding of limitations applied to the test.

Reconnaissance offers a plethora of options, each related to one another. However, unlike other phases within the test's framework, each option can be controlled, moderated, and measured to a surprisingly high level of granularity. Therefore, the relationship between the framework, tasks, and methods will become very clear.

## ENUMERATION

Enumeration (also known as network or vulnerability discovery) is essentially obtaining readily available (and sometimes provided) information directly from the target's systems, applications, and networks. An interesting point to make very early is that the enumeration phase represents a point within the project where the line between a passive attack and an active attack begins to blur. Without setting the appropriate expectations, this phase can have results ranging from "Oops" to "Do you swear to tell the truth and nothing but the truth?"

To build a picture of a company's environment there are several tools and techniques available to compile a list of information obtained from the systems. Most notably, port scanning is the "block and tackle" of the enumeration and NMap is today's most valuable player. The simplest explanation of a port scan is the manipulation of the basic communication setup between two networked systems using TCP/IP as a communication protocol. TCP/IP uses a basic session setup that can be used to determine what application ports a system is willing to use to establish communications.

Simply stated, port scanning is a way of detecting where a computer responds to requests to make connections. More technically, the TCP protocol has what is commonly known as the "three-way handshake" that is used to start TCP connections:

1. Computer A sends a message called a "SYN" (Synchronize) to Computer B.
2. Computer B acknowledges that message with a "SYN+ACK" (SYN with an Acknowledgement) to Computer A.
3. Computer A sends back an acknowledgement—"ACK."

Obviously, collecting information about systems is the first step in formulating an attack plan. However, information collected during the reconnaissance phase can be added to help build a picture of the target's systems and networks. It is one thing

