Penetration Testing Process

In the social sciences, a process is considered a term for the directed sequence of events. In an operational and organizational context, processes are referred to more precisely as work, business, production, or value creation processes. Processes are another name for programs running in computer systems, which are usually parts of the system software.

It is also essential to distinguish between `deterministic` and `stochastic` processes. A deterministic process is a process in which each state is causally dependent on and determined by other previous states and events. A stochastic process is one in which one state follows from other states only with a certain probability. Here, only statistical conditions can be assumed. For us, several of the above definitions overlap. We use the definition of the penetration testing process from the social sciences to represent `a course of events connected` with `deterministic processes`. This is because all of our steps are based on the events and results we can discover or provoke.

`A penetration testing process is defined by successive steps and events performed by the penetration tester to find a path to the predefined objective.`

Processes describe a specific sequence of operations within a particular time frame that leads to the desired result. It is also essential to note that processes do not represent a fixed recipe and are not a step-by-step guide. Our penetration testing processes must therefore be coarse and flexible. After all, every client has a unique infrastructure, desires, and expectations.

Penetration Testing Stages

The most effective way to represent and define these is through interdependent `stages`. We often find in our research that these processes are presented in the form of a circular process. If we look at this more closely and imagine that even a single component of the circular process does not apply, the entire process is disrupted. Strictly defined, the whole process fails. If we assume that we start this process from the beginning, but already with the newly acquired information, it is already a new process approach that does not undo the previous one.

The problem is that with these representations and approaches, there is often nothing to fall back on to extend our penetration testing process. As we have discussed, there is no step-by-step guide we can follow but `stages` that allow the individual steps and approaches to be flexibly varied and adapted to the results and information we receive. We can develop our own playbook for various things we try at different stages of a penetration test, but every environment is different, and thus, we need to adapt constantly.

We will go into each of these stages in more detail and cover the specifics of each in later sections and look at an `optional study plan` on how to proceed to learn the many Tactics, Techniques, and Procedures (TTPs), using a structure to show how each stage builds on the other and can also be iterative in nature. First, let's look at the broad components of the penetration testing process and discuss the individual modules and why they are so important.

This optional study plan is based on sets of modules for each stage that we recommend working through before moving on to the next stage. We will work through different phases in almost all of the modules, performing steps such as `Information Gathering`, `Lateral Movement`, and `Pillaging` repeatedly. The separation of the modules is designed to focus on the topic, which requires specific knowledge that should not be skipped. Gaps in any of this knowledge, even if we think we are familiar with it, can lead to misunderstandings or difficulties in the course of the study. Accordingly, the penetration testing process with its stages looks as follows:

Pre-Engagement

`Pre-engagement` is educating the client and adjusting the contract. All necessary tests and their components are strictly defined and contractually recorded. In a face-to-face meeting or conference call, many arrangements are made, such as:

- `Non-Disclosure Agreement`
- `Goals`
- `Scope`
- `Time Estimation`
- `Rules of Engagement`

Information Gathering

`Information gathering` describes how we obtain information about the necessary components in various ways. We search for information about the target company and the software and hardware in use to find potential security gaps that we may be able to leverage for a foothold.

Vulnerability Assessment

Once we get to the `Vulnerability Assessment` stage, we analyze the results from our `Information Gathering` stage, looking for known vulnerabilities in the systems, applications, and various versions of each to discover possible attack vectors. Vulnerability assessment is the evaluation of potential vulnerabilities, both manually and through automated means. This is used to determine the threat level and the susceptibility of a company's network infrastructure to cyber-attacks.

Exploitation

In the `Exploitation` stage, we use the results to test our attacks against the potential vectors and execute them against the target systems to gain initial access to those systems.

Post-Exploitation

At this stage of the penetration test, we already have access to the exploited machine and ensure that we still have access to it even if modifications and changes are made. During this phase, we may try to escalate our privileges to obtain the highest possible rights and hunt for sensitive data such as credentials or other data that the client is concerned with protecting (pillaging). Sometimes we perform post-exploitation to demonstrate to a client the impact of our access. Other times we perform post-exploitation as an input to the lateral movement process described next.

Lateral Movement

Lateral movement describes movement within the internal network of our target company to access additional hosts at the same or a higher privilege level. It is often an iterative process combined with post-exploitation activities until we reach our goal. For example, we gain a foothold on a web server, escalate privileges and find a password in the registry. We perform further enumeration and see that this password works to access a database server as a local admin user. From here, we can pillage sensitive data from the database and find other credentials to further our access deeper into the network. In this stage, we will typically use many techniques based on the information found on the exploited host or server.

Proof-of-Concept

In this stage, we document, step-by-step, the steps we took to achieve network compromise or some level of access. Our goal is to paint a picture of how we were able to chain together multiple weaknesses to reach our goal so they can see a clear picture of how each vulnerability fits in and help prioritize their remediation efforts. If we don't document our steps well, it's hard for the client to understand what we were able to do and, thus, makes their remediation efforts more difficult. If feasible, we could create one or more scripts to automate the steps we took to assist our client in reproducing our findings. We cover this in-depth in the `Documentation & Reporting` module.

Post-Engagement

During post-engagement, detailed documentation is prepared for both administrators and client company management to understand the severity of the vulnerabilities found. At this stage, we also clean up all traces of our actions on all hosts and servers. During this stage, we create the deliverables for our client, hold a report walkthrough meeting, and sometimes deliver an executive presentation to target company executives or their board of directors. Lastly, we will archive our testing data per our contractual obligations and company policy. We will typically retain this data for a set period or until we perform a post-remediation assessment (retest) to test the client's fixes.

Importance

We must internalize this procedure and use it as a basis for all our technical engagements. Each stage's components allow us to precisely understand which areas we need to improve upon and where most of our difficulties and gaps in knowledge are. For example, we can think of a website as a target we need to study.

Stage	Description
`1. Pre-Engagement`	The first step is to create all the necessary documents in the pre-engagement phase, discuss the assessment objectives, and clarify any questions.
`2. Information Gathering`	Once the pre-engagement activities are complete, we investigate the company's existing website we have been assigned to assess. We identify the technologies in use and learn how the web application functions.
`3. Vulnerability Assessment`	With this information, we can look for known vulnerabilities and investigate questionable features that may allow for unintended actions.
`4. Exploitation`	Once we have found potential vulnerabilities, we prepare our exploit code, tools, and environment and test the webserver for these potential vulnerabilities.
`5. Post-Exploitation`	Once we have successfully exploited the target, we jump into information gathering and examine the webserver from the inside. If we find sensitive information during this stage, we try to escalate our privileges (depending on the system and configurations).
`6. Lateral Movement`	If other servers and hosts in the internal network are in scope, we then try to move through the network and access other hosts and servers using the information we have gathered.
`7. Proof-of-Concept`	We create a proof-of-concept that proves that these vulnerabilities exist and potentially even automate the individual steps that trigger these vulnerabilities.
`8. Post-Engagement`	Finally, the documentation is completed and presented to our client as a formal report deliverable. Afterward, we may hold a report walkthrough meeting to clarify anything about our testing or results and provide any needed support to personnel tasked with remediating our findings.

Previous Next Mark Complete & Next

Table of Contents

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left