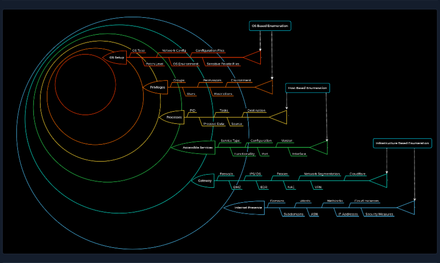
Enumeration Methodology

Complex processes must have a standardized methodology that helps us keep our bearings and avoid omitting any aspects by mistake. Especially with the variety of cases that the target systems can offer us, it is almost unpredictable how our approach should be designed. Therefore, most penetration testers follow their habits and the steps they feel most comfortable and familiar with. However, this is not a standardized methodology but rather an experience-based approach.

We know that penetration testing, and therefore enumeration, is a dynamic process. Consequently, we have developed a static enumeration methodology for external and internal penetration tests that includes free dynamics and allows for a wide range of changes and adaptations to the given environment. This methodology is nested in 6 layers and represents, metaphorically speaking, boundaries that we try to pass with the enumeration process. The whole enumeration process is divided into three different levels:

`Infrastructure-based enumeration` `Host-based enumeration` `OS-based enumeration`



Note: The components of each layer shown represent the main categories and not a full list of all the components to search for. Additionally, it must be mentioned here that the first and second layer (Internet Presence, Gateway) does not quite apply to the intranet, such as an Active Directory infrastructure. The layers for internal infrastructure will be covered in other modules.

Consider these lines as some kind of obstacle, like a wall, for example. What we do here is look around to find out where the entrance is, or the gap we can fit through, or climb over to get closer to our goal. Theoretically, it is also possible to go through the wall headfirst, but very often, it happens that the spot we have smashed the gap with a lot of effort and time with force does not bring us much because there is no entry at this point of the wall to pass on to the next wall.

These layers are designed as follows:

Layer	Description	Information Categories
`1. Internet Presence`	Identification of internet presence and externally accessible infrastructure.	Domains, Subdomains, vHosts, ASN, Netblocks, IP Addresses, Cloud Instances, Security Measures
`2. Gateway`	Identify the possible security measures to protect the company's external and internal infrastructure.	Firewalls, DMZ, IPS/IDS, EDR, Proxies, NAC, Network Segmentation, VPN, Cloudflare
`3. Accessible Services`	Identify accessible interfaces and services that are hosted externally or internally.	Service Type, Functionality, Configuration, Port, Version, Interface
`4. Processes`	Identify the internal processes, sources, and destinations associated with the services.	PID, Proceed Data, Tasks, Source, Destination
`5. Privileges`	Identification of the internal permissions and privileges to the accessible services.	Groups, Users, Permissions, Restrictions, Environment
`6. OS Setup`	Identification of the internal components and systems setup.	OS Type, Patch Level, Network config, OS Environment, Configuration files, sensitive private files

Important note: The human aspect and the information that can be obtained by employees using OSINT have been removed from the "Internet Presence" layer for simplicity.

We can finally imagine the entire penetration test in the form of a labyrinth where we have to identify the gaps and find the way to get us inside as quickly and effectively as possible. This type of labyrinth may look something like this:

The sqaures represent the gaps/vulnerabilities.

As we have probably already noticed, we can see that we will encounter one gap and very likely several. The interesting and very common fact is that not all the gaps we find can lead us inside. All penetration tests are limited in time, but we should always keep in mind that one belief that there is nearly always a way in. Even after a four-week penetration test, we cannot say 100% that there are no more vulnerabilities. Someone who has been studying the company for months and analyzing them will most likely have a much greater understanding of the applications and structure than we were able to gain within the few weeks we spent on the assessment. An excellent and recent example of this is the cyber attack on SolarWinds, which happened not too long ago. This is another excellent reason for a methodology that must exclude such cases.

Let us assume that we have been asked to perform an external "black box" penetration test. Once all the necessary contract items have been completely fulfilled, our penetration test will begin at the specified time.

Layer No.1: Internet Presence

The first layer we have to pass is the "Internet Presence" layer, where we focus on finding the targets we can investigate. If the scope in the contract allows us to look for additional hosts, this layer is even more critical than for fixed targets only. In this layer, we use different techniques to find domains, subdomains, netblocks, and many other components and information that present the presence of the company and its infrastructure on the Internet.

`The goal of this layer is to identify all possible target systems and interfaces that can be tested.`

Layer No.2: Gateway

Here we try to understand the interface of the reachable target, how it is protected, and where it is located in the network. Due to the diversity, different functionalities, and some particular procedures, we will go into more detail about this layer in other modules.

`The goal is to understand what we are dealing with and what we have to watch out for.`

Layer No.3: Accessible Services

In the case of accessible services, we examine each destination for all the services it offers. Each of these services has a specific purpose that has been installed for a particular reason by the administrator. Each service has certain functions, which therefore also lead to specific results. To work effectively with them, we need to know how they work. Otherwise, we need to learn to understand them.

`This layer aims to understand the reason and functionality of the target system and gain the necessary knowledge to communicate with it and exploit it for our purposes effectively.`

This is the part of enumeration we will mainly deal with in this module.

Layer No.4: Processes

Every time a command or function is executed, data is processed, whether entered by the user or generated by the system. This starts a process that has to perform specific tasks, and such tasks have at least one source and one target.

`The goal here is to understand these factors and identify the dependencies between them.`

Layer No.5: Privileges

Each service runs through a specific user in a particular group with permissions and privileges defined by the administrator or the system. These privileges often provide us with functions that administrators overlook. This often happens in Active Directory infrastructures and many other case-specific administration environments and servers where users are responsible for multiple administration areas.

`It is crucial to identify these and understand what is and is not possible with these privileges.`

Layer No.6: OS Setup

Here we collect information about the actual operating system and its setup using internal access. This gives us a good overview of the internal security of the systems and reflects the skills and capabilities of the company's administrative teams.

`The goal here is to see how the administrators manage the systems and what sensitive internal information we can glean from them.`

Enumeration Methodology in Practice

A methodology summarizes all systematic procedures in obtaining knowledge within the bounds of a given objective. It is important to note that a methodology is not a step-by-step guide but, as the definition implies, a summary of systematic procedures. In our case, the enumeration methodology is the systematic approach to explore a given target.

How the individual components are identified and information obtained in this methodology is a dynamic and growing aspect that is constantly changing and can therefore differ. An excellent example of this is using information-gathering tools from web servers. There are countless different tools for this, and each of them has a specific focus and therefore delivers individual results that differ from other applications. The goal, however, is the same. Thus, the collection of tools and commands is not part of the actual methodology but rather a cheat sheet that we can refer to using the commands and tools listed in given cases.

Powered by HACKTHEBOX