Phases of Hacking

There are mainly 5 phases in hacking. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It’s a stepwise process and when followed yields a better result.

Phases of hacking

1. Reconnaissance:

This is the first step of Hacking. It is also called as Footprinting and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,

Network

Host

People involved

There are two types of Footprinting:

Active: Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target

Passive: Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

1. Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

1. Gaining Access:

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

1. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

1. Clearing Track:

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.