**Topic: Hacking**

## WHO IS A HACKER?

In the computer security context, a **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in removing them. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community.

Hacking is usually a technical activity, although that does not necessarily mean that attackers are always technically capable. Most of the attackers are *script kiddies*, who know just about enough in order to use other (more competent) hackers' work. That fact aside, it is necessary to know the technical side of hacking, in order to understand the kind of knowledge that some attackers have. This section provides a brief explanation of how to get into a target system and how to exploit this as a full-scale hacking activity.

## CRACKING COMPUTER SYSTEMS

There are many ways for attackers to obtain illicit access to computer systems. This kind of access is often called "intrusion", and the first thing an intruder does is usually trying to obtain special/administrative privileges (a root access) on that system. Having a root access is very important for the attackers, since this means that they can do whatever they want on the system, including covering their tracks, strengthening their hold and doing damage.

In general, there are three main ways to intrude into a system:

- **Physical Intrusion**

This kind of intrusion happens when an intruder has a physical access to the target machine. This might allow the intruder to gain full control of the system – for example by booting with a special floppy or by taking the system apart physically (e.g. removing the Hard-drive to another system owned by the attacker, which then enables him/her to read/write to it).

- **System Intrusion**

In this case, it is assumed that the intruder has already got low-level privileges on the system. They then exploit un-patched security vulnerabilities in order to escalate their privileges to administrative level.

- **Remote Intrusion**

With remote intrusion, an attacker tries to get into the system remotely through the network. They initially do not have any privileges to the system, but one way or another – e.g. by finding out some valid account names and cracking their (usually weak) password, or by exploiting common security vulnerabilities (buffer overflow, etc.) – they manage to get in and obtain a root access.

This paper focuses on remote intrusion, as this is the most common type of attack associated with hackers. Nevertheless, there are some cases of system intrusion, for example, the insider attack, where a legitimate user (could be a disgruntled or former employee) performs an attack due to various reasons (revenge, cyber-espionage, etc.).

In order to minimize intrusion, many organizations install *Intrusion Detection Systems (IDS)*. Such a system inspects inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. There are many IDSs available. Most of these are commercial software and are primarily concerned with remote intrusion. We will not discuss IDS in great detail in this paper since our focus is on the attackers along with their hacking activities and some insights into their human aspects.

**TYPES OF ATTACKS**

Attackers can cause various levels of damage, depending on their skill level and/or their motives. There is a common pattern though: they usually follow a similar set of steps of information gathering before launching the attack.

**Foot Printing**

The aim of this activity is to obtain a complete profile of the target organization's network and its security arrangement. The information of interest includes the technology that the organization is using (e.g. Internet, Intranet, Remote Access, and Extranet) and its security policies and procedures. Although there are many different methods attackers can use to perform foot printing, there are four general steps that they are likely to follow: − Determine the scope of the foot printing activities. In some cases, it might be a bit too much to determine all entities associated to a Target organization. Therefore attackers often need to narrow down the scope of their Foot printing activities.

**Social Engineering**

Social Engineering is the term used to describe cracking techniques that rely on weaknesses in *wetware* (i.e. human users attached to the system – administrators, operators, etc.) rather than software. The aim is to trick people into revealing passwords or other information that compromises a target system's security.

**Software Bugs**

Another way to get into a system is through security vulnerabilities brought by bugs in the software (operating system, server daemons, client applications, etc.). It is almost impossible to have bug-free software and the attackers only need to find one hole in order to break in.

As a result, the program may crash and very often; this gives the attackers a root access and/or allows them to run any arbitrary code. Attackers can find buffer overflow bugs by:

1. browsing the web for known buffer overflow vulnerabilities on certain programs;
2. Searching for these bugs in the program directly if the source code is available;
3. Examining every place the program prompts for input and trying to overflow it with random (massive) data. If the program crashes, there is a chance that by carefully constructing the input, access to the system can be obtained.