1.8 Security Terminology

Security professionals have specific terminology. Individuals or system administrators who hold experience in network administration are most probably familiar with most of these terms. Although, most hacking terminology describes the activity or the person performing the action (phreaking, sneaker, etc.).

The first and most basic security device is the firewall. A firewall is a barrier between a network and the outside world. Sometimes a firewall is a stand-alone server, sometimes a router, and sometimes software running on a machine. Whatever its physical form, the purpose is the same (to filter traffic entering and exiting a network). Firewalls are related to, and often used in conjunction with, a proxy server. A proxy server hides your internal network IP addresses and presents a single IP address (its own) to the outside world.

Firewalls and proxy servers are added to networks to provide basic perimeter security. They filter incoming and outgoing network traffic but do not affect traffic on the network. Sometimes these devices are augmented by an intrusion-detection system (IDS). An IDS monitor’s traffic, which looks for suspicious activity that might indicate an attempted intrusion.

Access control is another important computer security term. Access control is the aggregate of all measures taken to limit access to resources. This includes logon procedures, encryption, and any method that is designed to prevent unauthorised personnel from accessing a resource. Authentication is clearly a subset of access control, perhaps the most basic security activity.

Authentication is the process of determining whether the credentials given by a user or another system (such as a username and password), are authorised to access the network resource in question. When a user logs in with a username and password, the system attempts to authenticate that username and password. If they are authenticated, the user will be granted access.

Non-repudiation is another term that is frequently encountered in computer security. This technique is used to ensure that the person performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides reliable records of which user took a particular action at a specific time. In short, it is methods to track what actions are taken by what user. Various system logs provide one method for non-repudiation. One of the most important security activities is auditing. Auditing is the process of reviewing logs, records, and procedures to determine whether they meet standards.

Least privilege is a concept you should keep in mind when assigning privileges to any user or device. The concept is that you only assign the minimum privileges required for that person to do his job, no more. Keep this simple but critical concept in mind.

You should also keep in mind the CIA triad, or Confidentiality, Integrity, and Availability. All security measures should affect one or more of these areas. For example, hard drive encryption and good passwords help protect confidentiality. Digital signatures help ensure integrity as well as a good backup system, or network server redundancy can also support availability.

1.8.1 Hacking Terminology

Please note that hacking terminology is not exactly accurate, and that many definitions can be debated. No “official” hacker vocabulary really exists. The terms evolve through their use within the hacker community. Let’s begin this examination by defining a hacker. A term used in movies and news broadcasts would be the most suitable starting point.

Most people use it to describe any person who breaks into a computer system. However, security professionals and hackers themselves use this term differently. In the hacking community, a hacker is an expert on a particular system or systems who wants to learn more about the system. Hackers feel that looking at a system’s flaws is the best way to learn about it.

For example, someone well versed in the Linux operating system who aims to understand that system by observing its weaknesses and flaws would be classed as a hacker. This “exploiting” part of the process is where hackers differentiate themselves into three groups:

- White hat hackers, upon finding vulnerability in a system, will report the vulnerability to the vendor of that system. For example, if they were to discover some flaw in Red Hat Linux, they would then e-mail the Red Hat company (probably anonymously) and explain what the flaw is and how it was exploited.
- Black hat hackers are the people normally depicted in the media (e.g., movies and news). After they gain access to a system, their goal is to cause some type of harm. They might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as crackers.
- Grey hat hackers are typically law-abiding citizens, but in some cases will venture into illegal activities. They might do so for a wide variety of reasons. Commonly, grey hat hackers conduct illegal activities for reasons they feel are ethical, such as hacking into a system belonging to a corporation that the hacker feels is engaged in unethical activities.