Hacking Terminology

Mark R. Adams, CISSP
KPMG LLP

Backdoor

Also referred to as a “trap door.” A hole in the security of a system deliberately left in place by designers or maintainers. Hackers may also leave back doors in systems they have compromised so they can return at a later time.

Banner Grabbing

The practice of obtaining the logon banners from target systems in order to find out what operating systems, versions, and patch levels they are running. This allows an attacker to focus his attack.

Brute Force

A method that relies on sheer computing power to try all possibilities until the solution to a problem is found.

Usually refers to cracking passwords by trying every possible combination of a particular key space.

Buffer Overflow

What happens when you try to stuff more data into a buffer (holding area) than it can handle. This problem is commonly exploited by crackers to get arbitrary commands executed by a program running with root permissions.

Chipping

Configuring processors or other computer chips so that they contain some unexpected functions. For example, they could be built so that they fail after a certain time, blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location.

DoS Attack

An abbreviation for “Denial of Service”, DoS refers to an attempt to shut down access to a particular system or network. The target is usually a high-profile web site or e-commerce site.

DDoS

An abbreviation for “Distributed Denial of Service”, DDoS refers to a coordinated DoS attack where a number of hosts are directed to attack a single target at the same time. The success of the attack is based on the large number of attacking hosts.

Logic Bomb

A bomb is a type of Trojan horse, used to release a virus, a worm or some other system attack. It's either an independent program or a piece of code that's been planted by a system developer or programmer.

Orange Book

Officially called the “Trusted Computer System Evaluation Criteria” (TCSEC) from the DoD. It presents the security requirements that a host must meet in order to be considered by the DoD a “trusted system.” There are various levels, ranging from “A” to “D”

C2 Security Level

Refers to a security rating of the Orange Book. Class C2 is titled “Controlled Access Protection,” and it refers to systems that make users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Red Book

Officially called the “Trusted Network Interpretation” (TNI) from the DoD. With the TNI, the security requirements and rating structure of the TCSEC are extended to networks of computers, ranging from local area networks to wide area networks.

Port Redirection

The process of redirecting network traffic from one IP address / port to another IP address / port. This is normal for firewalls and proxy servers, but hackers will sometimes do this in order to circumvent firewalls or secure ports.

Session Hijacking

A process where an attacker takes over, or "hijacks", an existing connection between a client and server. This allows that attacker to execute commands on the server as if he were the real client. Easily performed on Telnet sessions.

Spoofing

The process of impersonating another host on a network, including the Internet, by using that hosts IP or MAC address. This can enable the spoofer to mask an attack, or it can enable him to access another host with little or no authentication by pretending to be a “trusted” host.

Trojan Horse

A code fragment that hides inside a program and performs a disguised function. It's a popular mechanism for disguising a virus or a worm.

Virus

A code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces.

Worm

A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs.