

Internet Security Glossary of Terms

July 2007

A

Alert: Notification that a specific attack has been directed at a computer or network system.

Attack: Intentional act of attempting to bypass one or more computer or network security controls.

Authenticate: To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to an unauthorised user or unauthorised modification of data held on a computer system.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorisation to receive specific categories of information.

B

Back Door: Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door.

C

Countermeasures: Action, device, procedure, technique or other measure that reduces the vulnerability of a computer or network system.

D

Data Driven Attack: A form of attack that is encoded in seemingly innocuous data, which is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in

data form and launch an attack against a system behind the firewall.

Denial of Service: Result of any action or series of actions that prevents any part of an information system from functioning.

Dictionary Attack: An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.

Distributed Tool: A tool that can be distributed to multiple host machines, which can then be coordinated to anonymously perform an attack on the target host machine simultaneously after some time delay.

DNS Spoofing: Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

F

Firewall: A firewall is a hardware or software solution to enforce security policies. From a physical perspective, a firewall is equivalent to a lock on a door. It permits only authorised users such as those with a key or access card to enter. A firewall has built-in filters that block unauthorised or potentially dangerous material from entering the system. It also logs attempted intrusions.

Flooding: Type of incident involving insertion of a large volume of data resulting in denial of service.

Fact Sheet

H

Hacker: Unauthorised user who attempts to or gains access to an information system and the data it supports.

I

Intrusion: Unauthorised act of bypassing the security mechanisms of a system.

M

Malicious Code: Software capable of performing an unauthorized process on an information system.

Mobile Code: Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Malicious mobile code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorised information, corrupting information, denying service, or stealing resources.

P

Packet: A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Filtering: A feature incorporated into routers to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate email domains, and perform many other traffic control functions.

Packet Sniffer: A device or program that monitors the data travelling between computers on a network.

Probe: An attempt to gather information about an information system for the apparent purpose of circumventing its security controls.

Proxy: Software agent that performs a function or operation on behalf of another application or system while hiding the details involved.

R

Replicator: Any program that acts to produce copies of itself. Examples include; a program, a worm, or virus.

Retro-virus: A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

Rootkit: A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.

S

Smurfing: Software that mounts a denial of service attack by exploiting IP broadcast addressing and ICMP ping packets to cause flooding.

Spam: Indiscriminately sending unsolicited, unwanted, irrelevant or inappropriate messages, especially commercial advertising in mass



Fact Sheet

quantities, is considered spam. Another term used to describe spam is "electronic junk mail."

Spoofing: Impersonating another person or computer, usually by providing a false email name, URL or IP address.

T

Threat: Any circumstance or event with the potential to adversely impact an information system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.

V

Virus: Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

W

Worm: Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.