

# ExecutivePerils

11845 West Olympic Boulevard • Suite 795 • Los Angeles • CA • 90064  
T:310-444-9333 • F:310-444-9355 • Web: [www.eperils.com](http://www.eperils.com) • CA Lic# 0E36308  
dba: Executive Perils Insurance Services

## CYBER INSURANCE TERMS & DEFINITIONS

### **Ankle Biter**

A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to information systems. Usually associated with young teens that collect and use simple malicious programs obtained from the Internet.

### **Attack**

An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

### **Audit Trail**

In computer security systems, a chronological record of system resource usage. This includes user login, file access, security violations occurred, legitimate or unauthorized.

### **Back Door**

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door, a hidden software or hardware mechanism used to circumvent security controls. A secret way to enter a computer or program that bypasses normal operating mode.

### **Birthday attack**

Based on the statistical probability that finding two identical elements in a known finite space, the expected effort takes the square root of the key space number of steps. With only 23 people in a room, there is a better than even chance that two have the same birthday.

### **Bomb**

A general synonym for crash, normally of software or operating system failures.

### **Breach**

The successful defeat of security controls, which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

### **Brute force attack**

Typically a known plain text attack that exhausts all possible key combinations. Any key length above 94 bits is virtually infeasible to perform this attack.

# ExecutivePerils

## **Chernobyl packet (Kamikaze packet)**

A network packet that induces a broadcast storm and subsequent network meltdown. Typically an P datagram that passes through a gateway with both source and destination Enternet & IP Address set as the respective broadcast addresses for the subnet being gated between.

## **Chosen plaintext attack**

A cryptanalytic attack having chosen the associated plaintext for several ciphertext messages. A more powerful attack than Known-plaintext, because more information can be obtained to help deduce the key.

## **Ciphertext-only attack**

The cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm. The attacker is trying to recover the plaintext message or key.

## **Computer Network attack**

Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

## **Correlation attack**

Combining the output of several stream ciphertext sequences in some nonlinear manner. Thus revealing a correlation with the combined keystream and attacked using linear algebra.

## **Cracker**

A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security. Cracker: One who breaks security systems.

## **Cracking**

The act of breaking into a computer system. The act of breaking into a computer system or account; what a cracker does. Contrary to widespread myth, this does not usually persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems.

## **Craming**

A subtle scam used to get someone to change telephone long distance carriers without their knowledge.

## **Darkside hacker**

A criminal or malicious hacker, opposite of a white-hat hacker.

## **Data diddling**

The act of intentionally entering false information into a system or modifying existing data.

## **Data driven attack**

A form of attack that is encoded in innocuous seeming data that 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.

# ExecutivePerils

## **Data-in-motion attack**

An adversary's attempt to capture information while in transit, similar to man-in-the-middle-attack.

## **Demon dialer (see war dialer).**

A program, which repeatedly calls the same telephone number. This is benign and legitimate for access to a BBS or malicious when used as a denial of service attack.

## **Denial of service**

Action(s) that prevent any part of an information system from functioning in accordance with its intended purpose. Usually flooding a system to prevent it from servicing normal and legitimate requests.

## **Derf**

Gaining physical access to a computer that is currently logged in by an absent minded individual.

## **Dictionary attack**

Trying to discover a password by comparing a password file with a list of known hashed values of the password.

## **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.

## **Fork bomb (see Logic Bomb)**

Also known as Logic Bomb - Code that can be written in one line on any Unix system; used to recursively spawn copies of itself, "explodes" eventually eating all the process table entries and effectively locks up the system.

## **Hacker**

A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn the minimum necessary.

## **Hacking**

Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

## **Hijacking (IP)**

An action whereby an active, established, session is intercepted and co-opted by the unauthorized user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

## **Indirection**

Covering your tracks so that the target cannot identify or prove who is attacking them.

## **Internet worm**

A worm program that was unleashed on the Internet in 1988. Robert T. Morris wrote it as an experiment that got out of hand.

# ExecutivePerils

## **IP spoofing**

An attack whereby a system attempts to illicitly impersonate another system by using IP network address.

## **Joos**

An account where the user name and password are the same.

## **Known-plaintext attack**

The cryptanalyst has access not only to the ciphertext of several messages, and also the plaintext. The challenge is to deduce the key or keys used to encrypt or an algorithm to decrypt any new messages encrypted with the same key or keys.

## **Leapfrog attack**

Use of user-id and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

## **Letterbomb**

A piece of email containing live data intended to do malicious things to the recipient's machine 'or terminal. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service.

## **Logic bomb**

Also known as a Fork Bomb - A resident computer program which, when executed, checks for a particular condition or particular state of the system which, when satisfied, triggers the perpetration of an unauthorized act.

## **Mailbomb**

The mail sent to urge others to send massive amounts of email to a single system or person, with the intent to crash the recipient's system. Mailbombing is widely regarded as a serious offense.

## **Malicious code**

Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e.g. a Trojan horse.

## **Man-in-the-middle**

An active attack that typically is gaining information by sniffing or tapping a line between two unsuspecting parties.

## **NAK attack**

Negative acknowledgment . A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly leaving the system in an unprotected state during such interrupts.

## **Packet sniffing/filter**

A device or program that monitors data traveling between computers on a network.

## **Passive attack**

Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

# ExecutivePerils

## **Passive cheater**

The threat of unauthorized disclosure of information that doesn't change the state of the system. A type of threat that involves the interception, not the alteration, of information.

## **Perimeter security.**

The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters.

## **Piggyback attack**

Gaining unauthorized access to a system via another user's legitimate connection.

## **Ping -of-Death**

The use of Ping with a packet size higher than 65,507. This will cause a denial of service.

## **Port scanning**

A program that attempts to learn about the weaknesses of a computer or network edge device by repeatedly probing it with requests for information.

## **Retro-Virus**

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

## **Root kit**

A program that hackers implant in a victim's computer to hide their nefarious programs; 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. A root kit is a classic example of Trojan horse software and is available for a wide range of operating systems.

## **Session hijacking**

Taking over an open DTE / DOE session from someone who did not logout.

## **Shoulder Surf**

To look over someone's shoulder to view a pass phrase or pin to gain access at a later time.

## **Smurfing**

A denial of service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond en masse to the victim, clogging its network.

## **Sniffer / sniffing**

a program running on a computer or device that's attached to a network that filters, captures, and records network traffic, i.e. packets.

# ExecutivePerils

## **Spam**

A program to capture data across a computer network. Used by hackers to capture user ID names and passwords. Also a software tool that audits and identifies network traffic packets.

## **Spoofing**

Impersonating a server or person without permission. Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action. Attempt to gain access to a system by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

## **Superzapping**

The use of a utility program to modify information in computers. Leaving no trail of evidence, it circumvents the application from processing data or commands.

## **Threat**

The means by which to launch a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

## **Tripwire**

A software tool for security. Basically, it works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify it to the system security manager.

## **Trojan horse**

An apparently useful and innocent program containing additional hidden code, which allows the unauthorized collection, exploitation, falsification, or destruction of data.

## **Virus**

A program that can infect other programs by modifying them to possibly include an evolved copy of itself.

## **War dialer**

A program that will automatically dial a range of telephone numbers looking for a modem/computer to answer; a program that dials a given list or range of numbers and records those: which answer with handshake tones: or which might be entry points to computer or telecommunications systems.

## **White hat hacker**

One who usually does not break into unauthorized systems, but sometimes writes the tools that get used by the novices and black hats.

## **Whitemail**

The dissemination of false information for financial gain.

## **Worm**

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