**Privilege escalation** is the act of exploiting a [bug](http://en.wikipedia.org/wiki/Software_bug), design flaw or configuration oversight in an [operating system](http://en.wikipedia.org/wiki/Operating_system) or [software application](http://en.wikipedia.org/wiki/Software_application) to gain elevated access to [resources](http://en.wikipedia.org/wiki/Resource_(computer_science)) that are normally protected from an application or [user](http://en.wikipedia.org/wiki/User_(computing)).

**Hacking** means finding out weaknesses in a computer or computer network, though the term can also refer to someone with an advanced understanding of computers and computer networks.

[Password](http://www.wisegeek.com/how-often-should-i-change-my-password.htm) sniffing is a technique for harvesting passwords that involves monitoring traffic on a network to pull out information.

**Antivirus**  is [software](http://en.wikipedia.org/wiki/Software) used to prevent, detect and remove [malware](http://en.wikipedia.org/wiki/Malware), such as: [computer viruses](http://en.wikipedia.org/wiki/Computer_virus), [adware](http://en.wikipedia.org/wiki/Adware), [backdoors](http://en.wikipedia.org/wiki/Backdoor_(computing)), malicious [BHOs](http://en.wikipedia.org/wiki/Browser_Helper_Object), [dialers](http://en.wikipedia.org/wiki/Dialer), [fraudtools](http://en.wikipedia.org/wiki/Fraudtool" \o "Fraudtool),[hijackers](http://en.wikipedia.org/wiki/Browser_hijacking), [keyloggers](http://en.wikipedia.org/wiki/Keylogger" \o "Keylogger), malicious [LSPs](http://en.wikipedia.org/wiki/Layered_Service_Provider), [rootkits](http://en.wikipedia.org/wiki/Rootkit), [spyware](http://en.wikipedia.org/wiki/Spyware), [trojan horses](http://en.wikipedia.org/wiki/Trojan_horse_(computing)) and [worms](http://en.wikipedia.org/wiki/Computer_worm).

A **virus** is a small [infectious agent](http://en.wikipedia.org/wiki/Pathogen) that can replicate only inside the living cells of an organism. Viruses can infect all types of organisms, from [animals](http://en.wikipedia.org/wiki/Animal" \o "Animal)and [plants](http://en.wikipedia.org/wiki/Plant) to [bacteria](http://en.wikipedia.org/wiki/Bacteria) and [archaea](http://en.wikipedia.org/wiki/Archaea" \o "Archaea).[[1]](http://en.wikipedia.org/wiki/Virus#cite_note-pmid16984643-0)

A **backdoor** is a method of bypassing normal [authentication](http://en.wikipedia.org/wiki/Authentication), securing [remote access to](http://en.wikipedia.org/wiki/Backdoor_(computing)) a computer, obtaining access to [plaintext](http://en.wikipedia.org/wiki/Plaintext), and so on, while attempting to remain undetected.

An Internet proxy is an online computer server that acts as an intermediary between an Internet user and his destination site. Internet users use IP address to connect to the Internet.

A [computer](http://www.webopedia.com/TERM/R/retrovirus.html) retrovirus is one that actively seeks out an [antivirus program](http://www.webopedia.com/TERM/A/antivirus_program.html) on a [computer system](http://www.webopedia.com/TERM/C/computer_system.html) and attacks it. A retrovirus will attempt to disable and infect the antivirus [software](http://www.webopedia.com/TERM/S/software.html) in order to avoid detection in the computer system.

A **computer worm** is a standalone [malware](http://en.wikipedia.org/wiki/Malware) [computer program](http://en.wikipedia.org/wiki/Computer_program) that replicates itself in order to spread to other computers.

A **Trojan horse** is a type of [malware](http://en.wikipedia.org/wiki/Malware) that masquerades as a legitimate file or helpful program possibly with the purpose of granting a [hacker](http://en.wikipedia.org/wiki/Hacker_(computer_security)) unauthorized access to a computer.

The **man-in-the-middle** is a form of active [eavesdropping](http://en.wikipedia.org/wiki/Eavesdropping) in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

An [**intrusion detection system**](http://en.wikipedia.org/wiki/Intrusion_Detection_System) is a device or [software application](http://en.wikipedia.org/wiki/Software_application) that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station.