List of cybersecurity jargons

These are the types of cybersecurity jargons that attack a computer system or a network system, these include:

1. Authentication

The process of identifying a user’s identity, making sure that they can have access to the system and/or files. This can be accomplished either by a password, retina scan, or fingerprint scan, sometimes even a combination of the above.

1. Botnet

A combination of the words “robot” and “network”, a botnet is a network of computers that have been infected with a virus, and now are working continuously in order to create security breaches. These attacks come in the form of Bitcoin mining, sending spam e-mails, and DDoS attacks (see below).

1. Data Breach

The result of a hacker successfully breaking into a system, gaining control of its network and exposing its data, usually personal data covering items such as credit card numbers, bank account numbers, Social Security numbers, and more.

1. DDoS

The acronym stands for Distributed Denial of Service and is a favourite Black Hat tool. Using multiple hosts and users, hackers bombard a website with a tidal wave of requests to such an extent that it locks up the system and forces it to temporarily shut down.

1. Domain

A series of computers and associated peripherals (routers, printers, scanners), that are all connected as one entity.

1. Encryption

Coding used to protect your information from hackers. Think of it like the code cipher used to send a top-secret coded spy message.

1. Exploit

A means of attack on a computer system, either a series of commands, malicious software, or piece of infected data. Note that in this context, “exploit” is a noun, not a verb, as in “The hacker used a malware exploit to gain access to the credit card’s server.”

1. Firewall

Any technology, be it software or hardware, used to keep intruders out.

1. Hacker, Black Hat

Any hacker who attempts to gain unauthorized access to a system with the intent to cause mischief, damage, or theft. They can be motivated by greed, a political agenda, or simply boredom.

1. Hacker, White Hat

A hacker who is invited to test out computer systems and servers, looking for vulnerabilities, for the purposes of informing the host of where security needs to be buffed up. They are benign hackers, personifying the old axiom “It takes a thief to catch a thief”. Sometimes called ethical hackers

1. Malware

A portmanteau of “malicious” and “software”, describing a wide variety of bad software used to infect and/or damage a system. Ransomware, worms, viruses, and trojans are all considered malware. It most often delivered via spam emails.

1. Man in the Middle Attack

An attack on the “middleman”, in this case, defined as the Wi-Fi system that connects users to the Internet. Hackers who commit Man in the Middle Attacks can break the Wi-Fi’s encryption and use this as a means of stealing your personal data because they’re now in the system.

1. Phishing

A scam where a hacker poses as a legitimate business or organization (especially credit card companies, banks, charities, Internet providers, other utilities) in order to fool the victim into giving them sensitive personal information or inducing them to click a link or attachment that ends up delivering malware. Some of these schemes are extremely well done, others are sloppy and amateurish and can be spotted with just a little extra vigilance.

1. Ransomware

A form of malware that hijacks your system and encrypts your files, denying you access to them until you send money to unlock everything. In other words, it kidnaps your computer and holds it for ransom, hence the clever name.

1. Spoofing

Sadly, this has nothing to do with Weird Al Yankovic doing a parody version of a popular song. Rather, it’s when a hacker changes the IP address of an email so that it seems to come from a trusted source.

1. Spyware

A form of malware used by hackers to spy on you and your computer activities. If a mobile device such as a smartphone is infected with spyware, a hacker can read your text messages, redirect your phone calls, and even track down where you are physically located!

1. **Code Red** was a computer worm designed to exploit major flaws in Microsoft's Internet Information Services web server.
2. Trojan Horse

Yet another form of malware, this one a misleading computer program that looks innocent, but in fact allows the hacker into your system via a back door, allowing them to control your computer.

1. Virus

Malware which changes, corrupts, or destroys information, and is then passed on to other systems, usually by otherwise benign means (e.g. sending an email). In some cases, a virus can actually cause physical damage.

1. VPN

An acronym standing for Virtual Private Network, a VPN is a method of connecting a series of computers and devices in a private encrypted network, with each user’s IP address being replaced by the VPN’s IP address. Users get Internet anonymity, making it difficult for hackers to attack.

1. Worm

Malware that can reproduce itself for the purposes of spreading itself to other computers in the network. Particularly nasty, worms can either be simply a means of slowing down a system by eating up resources, or by committing exploits such as installing back doors or stealing data.

1. Cloud

You already utilize cloud computing if you use Gmail for email, Google Drive for document storage, or Netflix to stream your favourite movies. These services are all built on the cloud. [cloud computing](https://www.simplilearn.com/tutorials/cloud-computing-tutorial/what-is-cloud-computing) is providing on-demand services over the internet. If you want to run a business and you need to keep user data and you decide to do it on a hard drive, you will need a lot of storage space and a tech staff for it. Cloud service providers like Microsoft Azure, AWS, and Google Cloud, which offer on-demand services and are both cost-effective and low-risk in terms of security, make this procedure simple.

1. Software

It is a group of applications that instruct a computer to carry out a task. In which Users can download and use a package that contains these instructions a hard drive or magnetic diskette are common examples of external long-term memory devices where software is often kept. When it is in use the computer reads the program from the storage device and temporarily stores the instructions in random access memory (RAM). Google Chrome is one such example of application software.

1. IP Address

The world IP stands for Internet Protocol. An [IP address](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-an-ip-address) is a series of numbers allocated to computers routers  servers, and pretty much anything connected to the Internet, including websites. It functions very similarly to a standard address, allowing users to find any system or device on the global network by specifying its location

1. Rootkit

A rootkit is a collection of programs or software tools that allow hackers to remotely access and control a computer or network. Although rootkits do not directly damage users, they have been used for other purposes that are legal, such as remote end-user support. However, the majority of rootkits either leverage the system for additional network security attacks or open a backdoor on the targeted systems for the introduction of malware, viruses, and ransomware. Typically, a rootkit is installed without the victim's knowledge via a stolen password or by taking advantage of system flaws. In order to avoid being picked up by endpoint antivirus software, rootkits are typically employed in conjunction with other malware.

1. BYOD (Bring Your Own Device)

[Bring Your Own Device](https://www.simplilearn.com/what-is-byod-and-why-it-is-important-article) (BYOD) is a company policy that permits, encourages, or mandates employees to access enterprise systems and data using their own personal devices, such as laptops, tablets, and smartphones, for work-related activities.

1. Pen-testing

An approach to security evaluation where manual exploitations and automated techniques are used by attack and security professionals. Only environments with a solid security infrastructure should employ this advanced kind of security evaluation with a mature security infrastructure. Penetration tests can disrupt operations and harm systems because they employ the same equipment, procedures, and methodology as malicious hackers

1. Social Engineering

Instead of breaking in or utilizing technical hacking techniques, social engineering is a growingly popular way to access restricted resources. This strategy relies on user manipulation and human psychology. An employee might get an email from a social engineer purporting to be from the IT department in order to deceive him into disclosing private information rather than trying to uncover a software weakness in a company system. Spear phishing assaults are built on a foundation of social engineering.

1. Clickjacking

While someone is tricked into clicking on one object on a web page when they want to click on another, this practice is known as clickjacking. In this manner, the attacker is able to use the victim's click against them. Clickjacking can be used to enable the victim's webcam, install malware, or access one of their online accounts.

1. Deep fake

A piece of audio or video that has been altered and changed to make it seem authentic or credible. The most perilous aspect of the prevalence of deep fakes is that they can easily convince individuals into believing a particular tale or idea, which may lead to user behaviour that has a greater impact on society at large, such as in the political or financial spheres.

1. Multi-Factor Authentication

Multi-factor authentication (MFA), also referred to as two-factor authentication, makes it more difficult for hackers to access your account by requiring you to provide at least two different credentials. MFA requires a second factor to confirm your identity in addition to your username and password, such as a one-time security code, a fingerprint scan, or a face recognition scan.

1. User Authentication

A technique to prevent unauthorized users from accessing sensitive data is user authentication. For instance, User A can only see data that is relevant and cannot view User B's sensitive information.

1. Antivirus

The newest virus detection technology is integrated into anti-virus systems to shield users against viruses, spyware, Trojans, and worms that can damage computer hardware through email or web browsing.

1. Ethical Hacking

With the owner's permission, breaches the network to obtain sensitive information—completely legal. Typically, this technique is used to check for infrastructure weaknesses.

1. Cyber Attack

Any attempt to breach a logical environment's security boundary. An attack may concentrate on intelligence gathering, disrupting company operations, exploiting weaknesses, keeping track of targets, stopping work, obtaining value, harming logical or physical assets, or leveraging system resources to enable assaults against other targets.

1. Network

Two or more computers connected together to share resources (such printers and CDs), exchange files, or enable electronic communications make up a network. A network's connections to its computers can be made by cables, phone lines, radio waves, satellites, or infrared laser beams.

1. Internet of Things

The phrase "[Internet of Things](https://www.simplilearn.com/what-is-iot-how-and-why-it-matters-article)" (IoT) refers to commonplace items that are connected to the internet and are capable of autonomously collecting and transferring data without requiring human input. Any physical thing that can be given an IP address and can transport data is considered to be a part of the Internet of Things, which also includes traditional computers, vehicles, CCTV cameras, household appliances, and even people.

1. Penetration Test

A penetration test, commonly referred to as a pen test, simulates a cyberattack on your computer system to look for weaknesses that could be exploited. Pen testing involves attempting to get into any number of application systems (such as frontend/backend servers, APIs, etc.) in order to find security holes like unsensitised inputs that are vulnerable to code injection attacks.