VULNERABILITIES AND ATTACKS

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database.[citation needed] An exploitable vulnerability is one for which at least one working attack or exploit exists. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts. To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of these categories below

BACKDOOR
A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for many reasons, including by original design or poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Backdoors can be very hard to detect, and backdoors are usually discovered by someone who has access to application source code or intimate knowledge of the operating system of the computer.

DENIAL-OF-SERVICE ATTACK
Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.[17] Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

DIRECT-ACCESS-ATTACKS
An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless microphones. Even when the system is protected by standard security measures, these may be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

EAVESDROPPING
Eavesdropping is the act of surreptitiously listening to a private computer "conversation" (communication), typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the Federal Bureau of Investigation (FBI) and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped

upon via monitoring the faint electromagnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

PHISING

Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users.[20] Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose "look" and "feel" are almost identical to the legitimate one. The fake website often asks for personal information, such as log-in details and passwords. This information can then be used to gain access to the individual's real account on the real website. Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers are using creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices[21] to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized.

PRIVILEGE ESCALATION

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to exploit a vulnerability in the system to gain access to restricted data; or even become "root" and have full unrestricted access to a system.

REVERSE ENGINEERING

Reverse engineering is the process by which a man-made object is deconstructed to reveal its designs, code, architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon.

SIDE-CHANNEL ATTACK

Any computational system affects its environment in some form. This effect it has on its environment, includes a wide range of criteria, which can range from electromagnetic radiation, to residual effect on RAM cells which as a consequent make a Cold boot attack possible, to hardware implementation faults which allow for access and or guessing of other values that normally should be inaccessible. In Side-channel attack scenarios the attacker would gather such information about a system or network to guess its internal state, and as a result access the information which is assumed by the victim to be secure.

SOCIAL ENGINEERING

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access by, for example, impersonating a senior executive, bank, a contractor, or a customer.[23] This generally involves exploiting peoples trust, and relying on their cognitive biases. A common scam involves emails sent to accounting and finance department personnel, impersonating their CEO and urgently requesting some action. In early 2016, the FBI reported that such "business email compromise" (BEC) scams had cost US businesses more than $2 billion in about two years