Security Threats

The purpose of this document is to provide a basic overview of known security threats

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using fake bait in an attempt to catch a victim

Niagara Letter

Mails sent containing links containing software such as key loggers

Fake helpdesk calls to users

Hackers will call homes or business using directory, you will be coerced into going to a website that gives remotes access to your computer or server

Password attacks

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.

The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by System Administrators to check for easily crackable passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.

Denial of Service

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target

Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

Common forms of denial of service attacks are:

Buffer Overflow Attacks

The most common kind of DoS attack is simply to send more traffic to a network address than the programmers who planned its data buffers anticipated someone might send. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack in case it might work. A few of the better-known attacks based on the buffer characteristics of a program or system include:

•Sending e-mail messages that have attachments with 256-character file names to Netscape and Microsoft mail programs

•Sending oversized Internet Control Message Protocol (ICMP) packets (this is also known as the Packet Internet or Inter-Network Groper (PING) of death)

•Sending to a user of the Pine e-mail program a message with a "From" address larger than 256 characters

SYN Attack

When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first packet in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established. In general, this problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the timeout period.

Teardrop Attack

This type of denial of service attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.

Smurf Attack

In this attack, the perpetrator sends an IP ping (or "echo my message back to me") request to a receiving site The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. (Sending a packet with someone else's return address in it is called spoofing the return address.) The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

Viruses

Computer viruses, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targeted but simply a host unlucky enough to get the virus. Depending on the particular virus, the denial of service can be hardly noticeable ranging all the way through disastrous.

Physical Infrastructure Attacks

Here, someone may simply snip a fiber optic cable. This kind of attack is usually mitigated by the fact that traffic can sometimes quickly be rerouted.

References:

https://en.wikipedia.org/wiki/Phishing

https://en.wikipedia.org/wiki/Computer_worm

https://en.wikipedia.org/wiki/Computer_virus

https://en.wikipedia.org/wiki/Trojan_horse_(computing)

https://en.wikipedia.org/wiki/Denial-of-service_attack

http://www.cisco.com/c/en/us/products/security/annual_security_report.html