DIFFERENT TYPES OF SYSTEM VULNERABILITIES AND ATTACKS

Before you start

Objectives: Learn about different types of system exploitation attacks and which measures should be performed for protection.

Prerequisites: no prerequisites.

Key terms: software, access, buffer, system, back, overflow, attacker, control, type, attack, door

---

What is Back Door

Back Door is an access method which is not protected, and which is not monitored by our security system. Back doors can be used for legitimate actions, like updating software, servicing devices, etc. The problem with this type of feature is that it can be used by an attacker. Back door can also be implemented in a form of stand alone service or application which provides an unmonitored pathway into our secure environment. An example of that is a Trojan Horse. This type of malicious code gives an attacker abilities to control our system remotely and to gain access to our data. Back Door can also be in a form of a hardware device. Some devices may have available ports which can be used to connect to secure environment. Such ports can be, for example, console ports on routers which are used for router administration. An attacker can connect to the router device by using that port and then change or delete configuration.

To protect from this type of attack we should have very strict auditing measures implemented. Also, we should have antivirus software in our environment. We should have some sort of access control methodology. We should control our software deployment. Only legitimate software should be installed. Every default account on every device should be changed or disabled. We should also control access to important physical devices such as routers and servers.

Software Exploitation

In this type of attack, the attacker will exploit the vulnerabilities in software itself. This vulnerabilities might be mistakes in program code, and which can then cause problems with security. Attackers can discover those mistakes and then use them to gain access to the protected system.

Buffer Overflow

Buffer Overflow is actually an example of software exploitation attack. Buffer overflow can happen when a program doesn't have proper limitations implemented on how much or what type of data can be inputted into application. Buffer overflow can cause all sorts of problems, including Denial of Service (DoS), freezing, rebooting, achievement of unrestricted access, etc.

To protect from Buffer Overflow, programmers have to ensure software boundaries, so that the program doesn't process improper data. Intrusion detection system can be implemented to discover when a buffer overflow attack is being performed. Also, we can implement file system encryption, access control and auditing.

Source : http://www.utilizewindows.com/security/basics/410-different-types-of-system-vulnerabilities-and-attacks