Common Security Exploit and Vulnerability Matrix v2.0

Full-page infographic poster titled "Common Security Exploit and Vulnerability Matrix v2.0" produced by Tripwire, depicting an interconnected diagram of security services, applications, exploits, weaknesses, and files.

Matrix Key

Symbol	Meaning
Service or Application	
Information	
Exploit or weakness	
File	

What is a trojan horse?
An attacker might be able to replace certain programs and shared libraries. The replacement program is usually called a trojan horse. The trojan horse may emulate the original program so that the replacement goes undetected. The trojan may be able to sniff passwords, provide back door access, and even hide other programs from the system.

What is a rootkit?
A rootkit is a set or trojan horse programs that can be installed on a computer. These programs allow the attacker to hide themselves, files and logins from the system administrator. Furthermore, these programs usually leave back doors within the system. It is important to use integrity assessment tools to make sure that files have not been replaced, otherwise a rootkit can be very hard to detect.

What is a buffer overflow?
Software bugs exist when sufficient bounds checking is not performed on input. In this case, the program either crashes, or executes code unknown to the system. In the case it is possible to change the program by executing arbitrary code and obtaining remote root access. This is perhaps the most common type of bug, and potentially the most deadly. Buffer overflows are difficult to detect or prevent during software design. While the potential for more and varied software is ever increasing, the chance of software bugs also increases.

What is hijacking?
Because of the weaknesses of TCP/IP, it is vulnerable to spoofing and hijacking. Hijacking describes a special type of spoofing attack. Normal spoofing applications take place over a "session." If the session can be sniffed, or the sequence numbers can be guessed, the session can be "hijacked." The attacker can inject spoofed packets into the session stream and cause commands to be run as the original user.

What is spoofing?
The TCP/IP protocol has no authentication mechanisms. What this means is that anyone can create a "fake" packet and impersonate another host. On the other hand, if a machine is running a service and a false IP address. Many attacks can be executed using spoofed packets. Even if a victim logs all of the packets and uses intrusion-detection software, the source of a spoofed packet is impossible to determine. This makes catching the attacker very difficult. Additionally, some software that allows IP source address spoofing of the packet. Because IP can be spoofed, the program in question can sometimes be fooled into allowing access, running commands, etc.

What is excess privilege?
Sometimes software will be installed or run with too much power. An example might be a public server daemon running as 'root' (or SYSTEM in the case of Windows NT). Some programs require a complex and always have the potential of being exploited; administrators should lower the window of 'trust' and give processes only the power that they need to function. Anything in excess only increases the risk of total system compromise if the process is exploited.

What is change control?
Often, the largest threats to system stability and security are introduced by unauthorized changes, or the unexpected side effects of authorized changes. Change control is a combination of policies and procedures designed to restrict these risks. In mission-critical environments, change control is often based on a workflow requiring documenting requested changes, getting authorization from an authorized party and then implementing the authorized work order. However, change control can be as simple as announcing changes before you make them, and archiving those announcements.

What are "repeatable builds"?
Mission-critical functions must be able to survive the failure or destruction of the infrastructure that runs them. Unfortunately, years of undocumented and uncontrolled changes often make it impossible to reconstruct critical servers, routers, databases, etc. Worse, the only time you learn this is when that system has never been properly compromised, corrupted, or degraded and you must be able to reconstruct the "known good state" exists. Repeatable builds ensure that all servers can be duplicated and provisioned from scratch. Many organizations have made changes directly on production systems, but make changes to the build process, ensuring that changes propagate repeatable builds. (Also often called "provisioning".)

What is a loadable kernel module?
Loadable kernel modules are intended as an easier way of adding kernel functionality, to avoid having to recompile the kernel every time new functionality is added. The problem is that most kernel modules can be loaded with root privileges. Given this, attackers can inject their own modules into a running kernel, and reboot the machine.

What is 'compensating control'?
Procedures for management to periodically verify existence of segregation of duties. Whenever a computer-based process involves sensitive, valuable, or critical information, the system must include controls involving a separation of duties.

IP Packet / Network Key (bottom right)

- ConSeal PC Firewall
- PIX Firewall
- IP Header
- IP Packet
- ICMP
- Gauntlet Firewall 5.0
- Firewall-1
- Firewall-1 Session Agent
- expreserve
- Linux Kernel
- TCP packet
- tcpip stack
- RIP