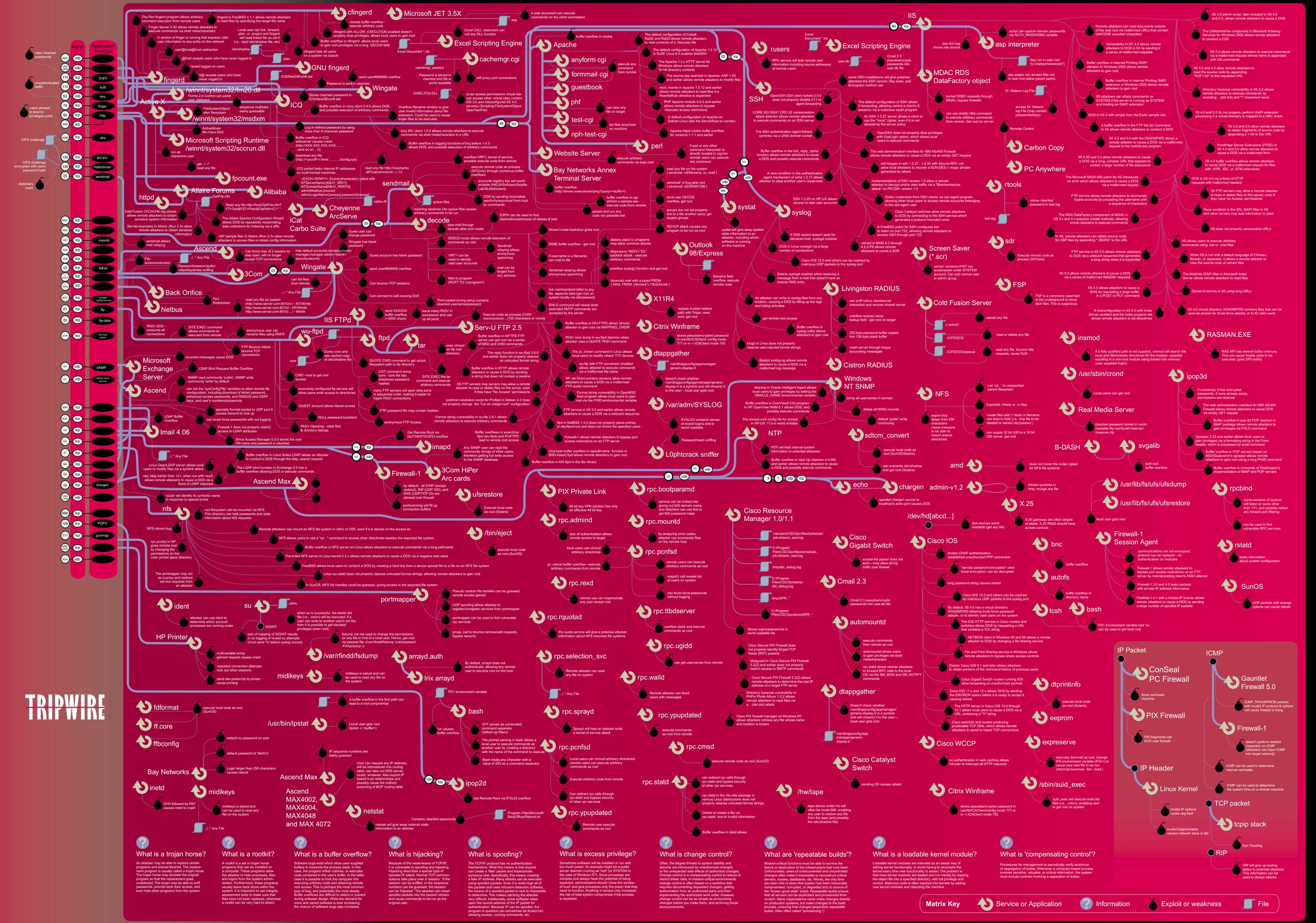
EC-Council CEH - Ethical Hacking and Countermeasures



What is a trojan horse?

An attacker may 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 processes, 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 which allow user-supplied buffers to overwrite the process stack. In this case, the program either crashes, or executes code contained in the user's buffer. In the latter case it is possible to trick the computer into 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 demand 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 spoofed IP attack. Normal TCP communications 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 insert 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 someone else. Specifically, this means creating a fake 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 next to impossible to determine. This makes catching the attacker very difficult. Additionally, some software relies upon the source address of the IP packet for authentication. 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). Since processes are complex and always have the potential of being exploited, administrators should 'close 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 compensating control to reduce or restrict these risks. In mission-critical environments, change control is often based on a workflow that requires 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 been irrevocably compromised, corrupted, or degraded and no source of the "known good state" exists. Repeatable builds ensure that all servers can be duplicated and provisioned from scratch. Many organizations never make changes directly on production systems, but make changes to the build process, ensuring that changes jeopardize 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 are loaded and run merely by copying the object file into a specified directory, with full privilege and control. Malicious code is often injected into kernels by adding new kernel modules and rebooting 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.

Matrix Key — Service or Application · Information · Exploit or weakness · File