Dr Hector Marco

Designing a secure working environment using multiple VirtualBox systems concurrently

Desktops and laptops computers are usually used to many things like check email, surf the web, edit documents, work with corporate applications, etc.

There are important differences when we are working with these applications. Not all applications have the same requirements in terms of connectivity but all are equally exposed to the network. For instance, a common attack vector is to exploit vulnerabilities in the browser client to finally access to the user data such us personal photos, emails or confidential documents.

This project propose the VirtualBox virtualisation as mechanism to isolate each task group. The idea is to have each group of tasks in a different virtual machine to prevent that an successful attack in a machine affects the others, and then limit the damage an attacker can make.

Thanks to the advances in virtualisation it is possible to friendly configure a desktop environment with multiple virtual machines running at the same time. This approach has multiple benefits such as the risks are separated, it is very easy and convenient restore back only the part affect of the system without stopping the other parts.

In practice, the use of this approach means that most of the attacks will not achieve their goal. For example, popular attacks like the Ransomware (malware that encrypt the user files and then demands a ransom payment to restore it) which typically uses the web browser or the email attack vector, simply will not have success because the user data is not in that virtual machine.

The work basically will consist on installing and configuring several virtual machines to build the proposed secure architecture. The results of this project are relevant because they are showing how to deal with real and unknown malware our society is facing.

Analysis of the MITRE's vulnerability databases. Trends and future evolution.

Computer security plays a key role in our society. Because of the huge amount of vulnerabilities reported every day, it is mandatory to organize, classify and uniquely identify every single vulnerability discovered around the world.

MITRE organisation, is organizing, enumerating (assigns an ID) and classifying vulnerabilities and exposures released by the cyber security researchers and vendors. This organization maintain a list of vulnerabilities, known as CVE (Common Vulnerability Exposures) and it plays a very real important role because it helps to avoid confusion and prevents duplications. This list is used by security professionals around the world, but also by hackers to build and/or
sell exploits.

The main purpose of this project is to become familiar with the information provided by the MITRE and get statistics that serve to analyse the evolution of the most common vulnerabilities, such as the attack vector, the operating system affected, etc.

The project consists basically in knowing how the vulnerabilities, and exposures are registered and to obtain statistics of the most relevant parameters. This statistics will provide valuable information helping maintainers and systems administrators to prioritize their efforts.

Using a Raspberry PI as a portable Firewall

With the internet expanding on a daily basis, old and new user's internet privacy and security become more vulnerable from multiple online threats. Unauthorized surveillance, cyber-attacks, ISP restrictions and censorship are examples of privacy and security leaks. Different efforts to improve these problems have been done by many initiatives. The suggested project consist on use a Raspberry PI device as a "plug and play" man in the middle device to mitigate Cyber threats. The idea is to use the Raspberry PI as a proxy but not only for HTTP but for all ports. The solution should be completely transparent as should provide some kind of mitigation mechanisms. For example, to use `iptables` to block some ports not commonly used or to log possible attack attempts. Additionally the system should be configured to run the minimum number of services to be less prone to attacks.