Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 13
HACKING CLOUDS

DRAFT

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Bob Monroe, ISECOM

Richard F. Abanto

Pablo Endres

ISECOM

Introduction

Wouldn't it be cool if you could have all of the different game consoles to be able to use the best one for each game? Well for many hackers, having a box (computer) running each of the different operating systems (each of them on different patch levels), applications and in some cases even different architectures (Sparc, x86, x86_64) has the same effect: having lots of toys to play with make Jack a happy boy.

Having this setup is really a pain and really expensive. Picture it in your head: 2-3 different PCs for Linux, 2-3 boxes for the different windows versions, maybe a couple of macbooks for macOSX, a Ultra10 for the Solaris 10 on Sparc. Everything setup on a couple of monitors and a big mess of tangled cables connecting it all. (I can hear my mom yelling at me already.)

Virtualization provides a great solution for this, you can have all of these machines running in one big server or even just the ones you need on your laptop. Each of these machines can run as a Virtual Machine or VM.

Now imagine you don't have to have the big server to all of this yourself, but all of them run somewhere in the Internet and you can access them when and where you want, better yet you can order a specific setup and have it available in a couple of minutes; use it, break it, trash it and pay a couple of cents for that.

This last picture is one of the services provided by cloud computing.

In this lesson we will talk about virtualization and cloud computing; what types of services can be provided and accessed, the infrastructure needed as well as that which is deployed, advantages and disadvantages and how it is used today.

Virtualization

According to NIST, Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM).[1]

This means that you can use specialized software to run other applications in it. In most cases what this means is that an isolation layer is added between the virtualized item and the actual machine.

Being the hacker domain that it is, you wouldn't expect only one type of virtualization to exist, right? So here are some well-known virtual machines or virtualization software which represent the different types that exist:

1. The Java Virtual Machine is a form of application virtualization; it provides an isolation layer between the application and the OS. Here the application should only be able to use the API provided by the virtual machine.

2. VMware with its multiple products, ~~SUN's~~ Oracle's Virtualbox or the Linux KVM are examples of full virtualization. They provide a container with virtual hardware where the OS and its applications run natively, which is called a virtual machine (VM).

3. Solaris Containers are an example of OS virtualization. It provides a virtual implementation of the OS interface that can be used to separate applications into different VM containers. This technology allows you to run multiple copies of the same OS, but you only have to maintain and patch the underlying version.

1 NIST **800-125: Guide to Security for Full Virtualization Technologies**

These virtualization technologies provide an isolation layer or container to run applications and / or operating systems in a contained environment. In many cases they also provide additional tools, like snapshots, cloning, migration; that make hacking a lot easier and fun.

Full Virtualization

In full virtualization, one or more OSs and the applications they contain are run in a container that presents full set of hardware: CPU, RAM, HDD, network interfaces.

Each instance of an OS and its applications runs in a separate VM called a guest operating system. The guest OSs on a host are managed by the hypervisor, also called the virtual machine monitor (VMM), which controls the flow of instructions between the guest OSs and the physical hardware.

The hypervisor is responsible for providing some level of isolation between the VMs and the hardware. It can partition the resources and can enable access to shared resources, including files or a printer.

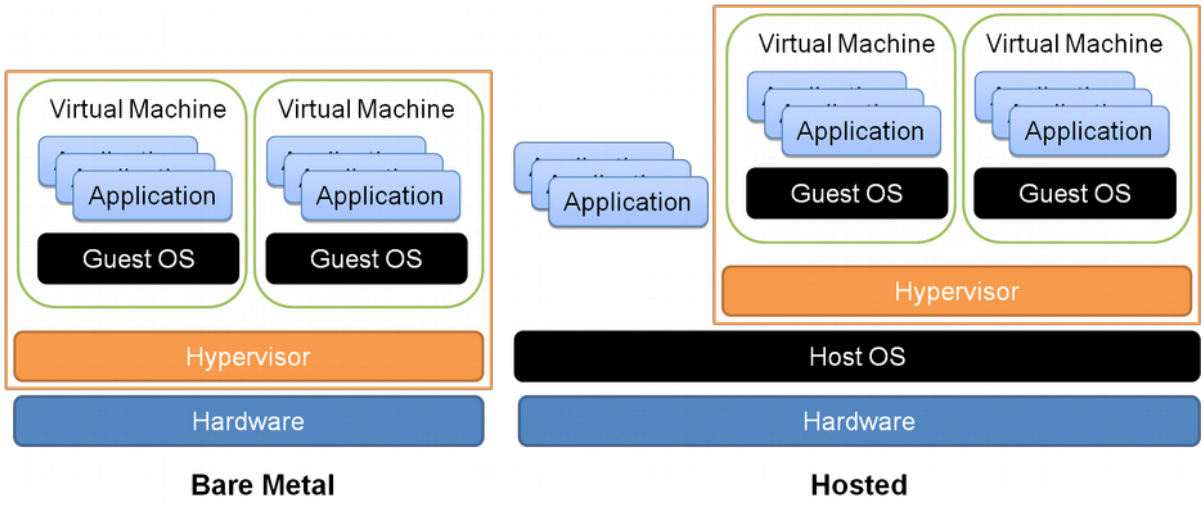
Two types of full virtualization exist, see Figure 1:

1.Bare metal: were the hypervisor runs directly on the hardware. Examples of this would be Red Hat Enterprise Virtualization (RHEV), Ubuntu's XXX or Vmware's ESXi.

This type of virtualization is normally used in a server environment, because your hardware is dedicated to virtualization.

2.Hosted: The hypervisor is run as an application on a host OS. Examples of this would be ~~SUN's~~ Oracle's Virtualbox, the Linux KVM or Vmware's Workstation.

This would probably a solution you could use in class or at home, because it runs on top of your OS.



Virtualization in everyday lives

Virtualization has made its way into all many realms of modern computing and in many cases makes our lives a lot easier.

App developers for mobiles devices use virtual machines to test their code without running it in each separate hardware platform; you can even test it on different Android versions. That means that the developers don't really need to have every model of phone in the market to test their App, considering how many different Android phones are out there, this is a great relief.

Since we are talking about Android, is this a form of virtualization? If so, what type?

In order to study for a certification, it is common to setup a lab environment to test the configuration. Since not everyone has a couple of switches and routers laying around home to study, there is a virtualization software that lets you model a complete setup including the network connections between the devices!

Malware experts use virtual machines to be able to set a virus loose in a contained environment and figure out how it works. It allows them to just search for the differences between before and after, they can even use it TiVo style: by pausing it, going back and seeing what instructions are being run in real-time.

Exercises:

A.Fire up your virtualization software and run a Linux machine. How can you notice from the inside that it is a virtual machine?
B.Try installing a hypervisor and guest OS inside a virtual machine, let's say: Linux, Virtualbox, Windows, Virtualbox, Linux. Does it work?

What is Cloud Computing?

Cloud Computing is an evolving model, which means that many definitions of the term exist. Basically, the term *Cloud Computing* is born from *Cloud*, referring to networks, in particular Internet; and *computing* that refers to the processing, storage, applications, services and hardware information infrastructure.

Figure 1: Cloud Computing.

Cloud Computing is a model that enables network access, i.e. via the Internet, to a set of computer services (networks, servers, storage, applications and services) conveniently and on demand (use only what you need).

A simple example of using cloud computing is the use of the services offered by Google. Take Gmail (Google Email), to access Gmail just need a browser (for PCs) or an App (for smartphones and tablets) to check our e-mail, send messages and more without the need to have them in our own local computer or device, because everything is stored and processed in the cloud (internet).

Exercises:

A.Search the Web for three different cloud providers
B.What makes you think that they are cloud providers and not just web sites?

Cloud Computing can be considered the result of throwing traditional hosting model and full virtualization in a box and shaking it really hard. It gives you almost instant access (you may have to wait 10-15 minutes for a VM to be usable) to unlimited compute resources.

In the next sections we will take about the characteristics of the different types of *Cloud Computing*.

Characteristics or Features of Cloud Computing

Cloud computing is the result of the evolution of a series of technologies, including virtualization, and the hosting model. The main five characteristics of Cloud Computing are:

- **On-demand self-service**: A consumer can provision and configure resources and services as needed without requiring human interaction with each service's provider.

- **Broad network access**: the customer can access the services over different networks, i.e. the Internet, and from different devices (PC, smartphone, table) and applications (Web based, PC application, App)
- **Resource pooling or sharing:** Providers have a set of physical resources are shared with multiple customers and are managed according to the demand. The location and architecture vendor hardware devices are generally not controlled by the client.
- **Rapid elasticity or scalability:** Resources can be increased or decreased depending on the needs of even automated depending on demand. To the customer, the recourses often appear to be unlimited i.e. the size of the mailboxes in Gmail.
- **Monitoring and metering:** given the flexibility of the services and the billing model (pay per use), it is essential that tools are in place to provide transparent and accurate monitoring and metering. In most cases a user can see his usage and costs in real-time.

Security is not one of the explicit characteristics of Cloud Computing. But this feature is very important. Providers should implement strict and transparent security policies that ensure the availability and confidentiality of data. For example, the Ubuntu One file service does not provide encryption for the files stored in it, but advises the users to use encfs.

It is important to have in mind, what happens in the Internet, stays in the Internet. So make sure you understand: what are the terms of the service you are signing up for, what your rights are and especially which rights are you granting the service provider.

Exercises:

1. Find the security and privacy policies of three cloud based file synchronization services.
2. Compare some of the basic issues:
    3. Are the files encrypted?
    4. What methods are used to encrypt network transfer and file storage?
    5. What about the ownership? Is the contents of the files yours or are you granting rights to the provider?
    6. Is data encrypted while transmitted?

Deployment Models

1. **Public:** Anyone can be a use of resources. To others it is shared.

Advantages	Cons
Scalability.	Infrastructure shared with other users and organizations.
Resource efficiency through pay-per-use models.	Lack of transparency for the customer, as no one knows the other services that share resources, storage, etc.
Most services enable collaboration over the Internet	Terms of service and privacy must be read in detail

2. **Private:** Are generally created for private companies, which give value to the service they provide.

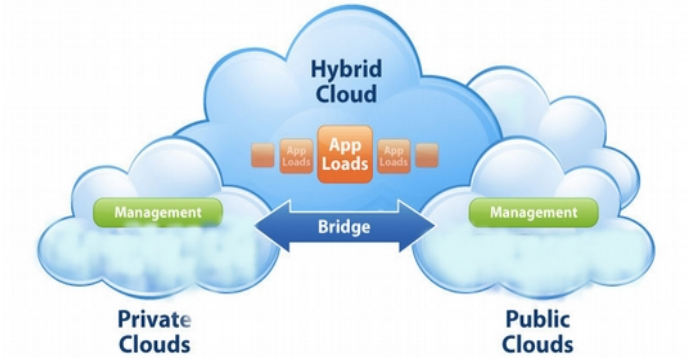
Advantages	Cons
Compliance with internal policies.	High material cost.
Ease of collaborative work between distributed sites.	Unit contracted infrastructure.
Full control of resources.	Slow return on investment given its internal service.

3. **Community:** Services are shared between multiple organizations with a shared concerns, i.e. compliance and security requirements, mission, etc

Advantages	Cons
Compliance with internal policies.	Host-dependent security infrastructure.
Reduce costs by sharing infrastructure and resources.	Unit contracted infrastructure.
Fast return on investment.	

4. **Hybrid:** This infrastructure is built by combining two or more of the models above (public, private or community) with a technology that provides compatibility.

Figure 2: hybrid cloud



Type of Services

In general term, the type of service depends on how much of the service has been outsourced or managed by the provider.

5.1 Software as a Service (SaaS): This is a software deployment in which applications and computing resources are designed to be offered as services on demand operation. The can normally be accessed from thin clients, i.e. web browser.

Generally the user cannot manage or administer the service, with the possible exception of user-specific application settings, i.e. language, look & feel, etc

5.2 Platform as a Service (PaaS): The consumer can deploy its own applications (acquired or self-built) using the programming languages and tools supported by the provider.

In this case the consumer can manage the deployed application and possibly the hosting environment configuration, but not operating system, storage, network, etc.

5.3 Infrastructure as a Service (IaaS): The capability is provided to the user to provision the computing infrastructure (servers, storage, software and network equipment) on demand.

The consumer does not manage the cloud infrastructure, but has control over the operating system, storage, applications and in some cases limited control of network components, i.e. a host firewall.

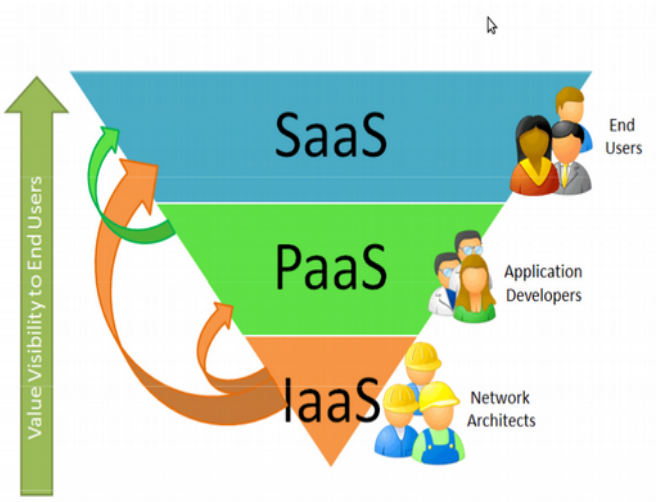


Figure 3: Cloud service models

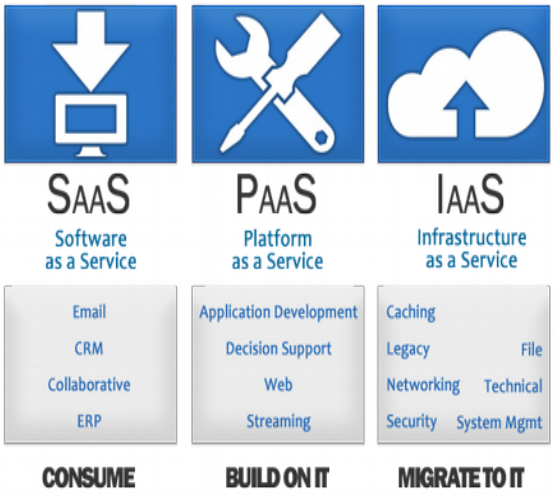


Figure 4: Applications depending on the type of cloud service used

Exercises:

- Search the Internet for three different SaaS offerings
- Search the Internet for three different PaaS offerings

- Search the Internet for three different IaaS offerings
- What is the main difference between these offerings?

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM