Types of Attacks and Security Methods. Virtual Machines

Dorina-Luminița COPACI[1], Constantin-Alexandru COPACI[2]
[1] Associate Professor, University Politehnica Bucharest - ETTI, Bucharest, Romania
lcopaci@yahoo.com
[2] Student, Titu Maiorescu University, Faculty of Informatics, Bucharest, Romania
copacialexandru8@gmail.com

Abstract

Virtualization is a type of process used to create a virtual environment. Many organizations think about the security implications after implementing a new technology. Virtualization can be used in many ways and requires appropriate security controls in each situation. This paper presents the idea of using a virtual machine to share services and information over the Internet. In case of an attack, the resources of the virtual machine will be affected, while the resources of the real machine are safe. In this paper, we present the perspective of an attack by running malicious software on a virtual machine. We will show that although unauthorized control of the virtual machine is obtained, the real machine is not affected.

Index terms: attack, security, Virtualization, virtual machine, VMware Workstation

1. Introduction

The introduction of computers into virtually every dimension of society has significantly changed the way people and organizations obtain or disseminate information or conduct business, allowing for greater efficiency, increased operational control, and efficient access to information. Along with many benefits, however, computers and their interconnection also present negative aspects, such as the emergence of new types of crimes (for example, the distribution of computer viruses), as well as the possibility of committing traditional crimes through new technologies (to for example, fraud or forgery). Since attacks on information systems can produce a series of negative consequences - financial, operational, legal, or strategic - at an individual, organizational or even national level, the risk of an attack must be well understood in order to be mitigated or eliminated [1].

In this paper we propose to discuss the types of electronic attacks, as well as methods of securing computer systems. We present the idea of using a virtual machine [6], [7] to protect real machine resources after a network attack. Thus, an attacker will attack the virtual machine that is installed on top of the real machine. In section 2 we present the concept of virtual machine. In this part of the work, we describe the VMware Workstation. Section 3 presents some of the types of attacks. The security methods are presented in section 4, to be exemplified by a case study. In the last section, we present our conclusions as a result of the study done for the realization of the work.

2. The concept of virtual machine

A virtual machine (VM) is an operating system (OS) or application environment that is installed on software, which imitates dedicated hardware [5]. A virtual machine provides an isolated

environment for running its own OS and applications independently from the underlying host system or from other VMs on that host. The virtual machine depends on the physical resources of the host. These resources are virtualized and distributed on the virtual machine and can be reallocated as needed so that it is possible to run different environments simultaneously and adapt workloads.

Advantages of the virtual machine:

- Partitioning – multiple applications and operating systems in one machine;
- Isolation – each virtual machine works in isolation from the hosts and from the other virtual machines;
- Encapsulation – every state of a virtual machine is contained in software, with standard virtual hard drives guaranteeing compatibility.

Types of Virtual Machine [7]:

1. System Virtual Machines — Hardware Virtual Machines

This provides an environment with the execution of separate complete operating system. Examples of this type of virtual machines are: VMWare, VirtualBox

2. Process Virtual Machines — Application Virtual Machines

This provides platform independent programming environment that abstract away details of the underlying hardware from software. Ex: .NET Framework, Java Virtual Machine.

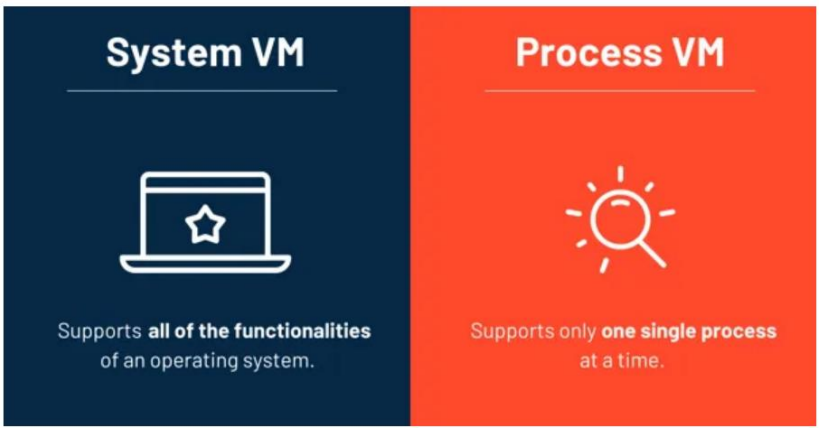

Fig. 1. Types of Virtual Machines [7]

2.1. VMware Workstation

Workstation is powerful desktop virtualization software for software developers/testers and enterprise IT professionals that runs multiple operating systems simultaneously on a single PC.

VMware [8], [10] refers to the computer and operating-system instance that executes the VMware Workstation process as the host machine, and identifies instances of operating systems running inside a virtual machine as guest virtual machines.

Like an emulator, VMware Workstation provides a completely virtualized set of hardware to the guest operating system — for example, regardless of make and model of the physical network adapter, the guest machine will see an AMD PC-net network adapter.

VMware [9], [10] virtualizes all devices within the virtual environment, including the video adapter, network adapter, and hard disk adapters. It also provides pass-through drivers for USB, serial, and parallel devices.

3. Types of attacks

Attacks on information in computer systems can take different forms.

A first classification of attacks can be made taking into account the place from where the attack is executed. We distinguish two categories of attacks: local and remote.

A second classification can be made according to the way the attacker interacts with the information resulting from a successful attack. Here two categories of attacks are distinguished: passive and active.

There are two main categories of attacks [14]: passive attacks (data interception) (Figure 2) and active attacks (data flow interruption, data modification and disinformation) (Figure 3).

a. The passive attacks are characterized by: they violate the confidentiality rules; they do not generate damages (do not delete or modify the data); transmitted data are intercepted using tapping wires, electromagnetic radiation interception, etc.
b. The active attacks are more dangerous, because they modify the status of data, computers or communication systems. There are the following main types of active attacks:
    - *Interruption* – uses the replay of a message or of a part of a message in or der to produce an unauthorized access.
    - *Modification* - represents an attack that modifies (through insertion and/or deletion of characters) a part or all transmitted data.
    - *Disinformation* – represents a type of attack where an unauthorized user pretends that is an authorized user.

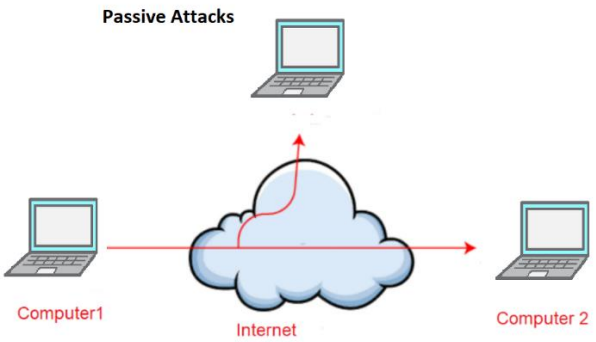

Fig. 2. Passive Attacks

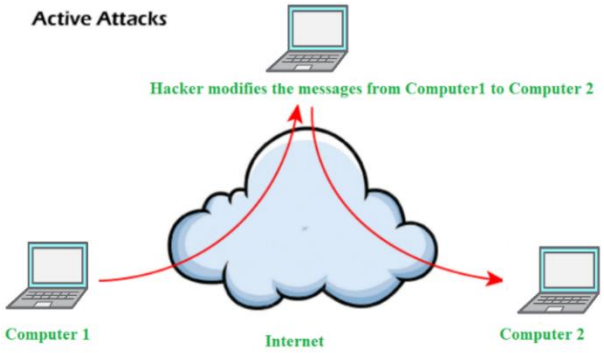

Fig. 3. Active Attacks

3.1. Examples of attacks

DOS attack

A denial-of-service attack (DoS attack) [11] is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. A DoS attack can be perpetrated in a number of ways.

There are three basic types of attack: consumption of computational resources, such as bandwidth, disk space, or CPU time; disruption of configuration information, such as routing information; disruption of physical network components. Examples of DOS attack: SYN flood attack, Fraggle attack, Ping of death attack, Distributed Denial of Service attack etc.

Viruses attack

In computer security, a computer virus is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of a virus into the program is termed as an "infection", and the infected file, or executable code that is not part of a file, is called a "host".

Viruses are one of the several types of malicious software or malware. In common parlance, the term *virus* is often extended to refer to worms, trojan horses and other sorts of malware; viruses in the narrow sense of the word are less common than they used to be, compared to other forms of malware. Examples of viruses attack: Companion viruses, Resident viruses, Nonresident viruses etc.

Trojan attack

In the context of computer software, a Trojan horse is a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

Backdoor attack

A backdoor [13] in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be a modification to a legitimate program.

Buffer overflow

In computer security and programming, a buffer overflow [1] is an anomalous condition where a process attempts to store data beyond the boundaries of a buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

E-mail spoofing

E-mail spoofing [12] is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. This involves changing certain properties of the e-mail, such as the *From*, *Return-Path* and *Reply-To* fields (which can be found in the message header) to make the e-mail appear to be from someone other than the actual sender.

4. Security methods

The security model for a system (a computer or a network of computers) can be seen as having several layers that represent the levels of security surrounding the subject to be protected. Each level isolates the subject and makes it more difficult to access it in any other way than it was intended.

Physical security represents the outer level of the security model and generally consists of locking computer equipment in an office or other premises as well as ensuring security and access control. Logical security consists of those logical methods (software) that ensure access control to system resources and services. It, in turn, has several levels divided into two large groups: access security levels and service security levels. Among the security methods of a system, we mention:

Virtual private networks

A Virtual Private Network (VPN) provides a way to establish secure communications over an otherwise insecure network. With the help of a VPN connection, the two sides of a connection can communicate under the same security conditions as those provided by a company's local network.

Firewall

Firewalls are used to protect/isolate segments of an extended network (eg the Internet), but especially to protect the private networks (Intranet) of a company/institution/bank/etc connected to the Internet. In what follows, by internal network we will refer to the network segment that must be

protected, respectively by external network we will refer to the network segment from where the threats can originate and over which we have no control (usually the rest of the Internet).

Antivirus programs

Antivirus programs must be chosen so that they have as large a database as possible with the definitions of known viruses in order to effectively protect the system, occupy as little memory as possible when monitoring computer activity and update themselves on the Internet as often as possible.

4.1. Case study. Practical example

We installed VMware Workstation on two operating systems: Windows and Linux. Then we installed the Windows 10 and Linux Red Hat 9.0 operating systems on the virtual machine [4].

We will try to attack both operating systems on the virtual machine to see if the local machine resources will be affected.

4.1.1. Security methods against a DOS attack

For a Denial-of-Service attack we use a program which was written for a Linux machine with a kernel patch in place to allow IP source address spoofing.

This program scans a host to determine which ports are open, or listening for connections. Once a list of receiving ports has been compiled, the program then floods each of them with the specified number of SYN packets.

When a TCP/IP stack receives a SYN packet, it responds with a SYN/ACK. At this point, it is waiting for an ACK. Now, if the source address in the SYN packet does not exist, but has a path to it in place, that SYN/ACK will never be answered with an ACK, and the TCP/IP stack will wait forever for that packet (actually until a certain amount of time has passed which is implementation-dependent). If a whole bunch of those faked SYN packets are received simultaneously, the connection queue of the target machine will he filled.

We can set the network connection to a virtual machine in three ways:

- Bridged – connected directly to the physical network;
- NAT – used to share the host's IP address;
- Host-only – a private network shared with the host.

If we chose to set up the network connection bridged, the virtual machine we'll use a different IP address from the real machine, and the bandwidth will be partly affected in case of a DOS attack over the virtual machine.

So, if we want that the local machine bandwidth not to be affected, we'll have to install a net limiter to divide the bandwidth in two: one for the virtual machine IP and one for the real machine IP. When the virtual machine IP will be flooded, half of the bandwidth will be affected, but the second half of the bandwidth will not be affected. In this way the real machine resources will not be affected.

If we chose to set up the network connection NAT, the virtual machine will use the same IP address as the real machine. In this case, if a DOS attack will affect the virtual machine, the real machine will be affected too. The real machine bandwidth will be affected.

So, if we want that the real machine resources not to be affected after a DOS attack, we must set the network connection bridged and then to use a net limiter to limit the bandwidth for the virtual machine IP address.

Otherwise, we can create a strong firewall on the virtual OS. We must set the firewall to drop the packets in case of a flood. In a Linux operating system [3], we can use the *iptables* command to drop the packets in case of a DOS attack.

4.1.2. Security methods against a buffer overflow attack

To create a buffer overflow attack [1], we first accessed the virtual machine with a Trojan horse. We inserted programs [3] into the virtual operating system with the intention of creating buffer overflows and then executed them.

We observed that this attack can destroy certain services or affect the memory allocated for the virtual machine, but the memory of the real machine remains unaffected. Therefore, the buffer overflow attack on the virtual machine has no effect on the resources of the real machine.

5. Conclusions

In this paper we wanted to study the situation in which, having installed a virtual machine on a real machine and attacking this machine, what is the probability that the resources of the real machine will be affected.

We analyzed some of the important types of attacks in a network, such as: DoS attacks, viruses, Trojans, backdoors, buffer overflow. After this analysis it was concluded that the probability of the real machine resources being infected in the event of an attack is very small. If the attack on the virtual machine represented a threat to the resources of the real machine, we presented in the paper solutions to remedy the problem.

Therefore, the resources of the real machine will be safe after an attack on the virtual machine if the instructions in the work are used.

References

[1]. Bernaschi, M., Grabrielli, E., Mancini, L. (2000) “Operating System Enhancements to Prevent the Misuse of System Calls”, Proceedings of the ACM Conference on Computer and Communications Security.

[2]. Bernaschi, M., Grabrielli, E., Mancini, L. (2002) “REMUS: A Security-Enhanced Operating System”,ACM Transactions on Information and System Security, Vol 5, 2001,

[3]. Blunden, B. (2002) “Virtual Machine Design and Implementation in C/C++”, Wordware Publ. Plano,Texas – USA.

[4]. Chen, P., Noble, B. (2001) “When Virtual Is Better Than Real”, Proceedings of the 2001 Workshop on Hot Topics in Operating Systems (HotOS).

[5]. Goldberg, R. (1973) “Architecture of Virtual Machines”, AFIPS National Computer Conference. New York – NY– USA.

[6]. *Oliphant,P., "Virtual Machines". Virtual Computing. Archived from the original on 2016-07-29*. Retrieved 2015-09-23.

[7]. Randika, Y., “Virtual Machines”, Feb 28, 2021, https://yasirurandika.medium.com/virtual-machines-937c99156ca5.

[8]. Sugerman, J., Ganesh, V., Beng-Hong L. (2001). Virtualizing I/O Devices on VMware Workstation’s Hosted Virtual Machine Monitor. Proceedings of the 2001 USENIX Annual Technical Conference.

[9]. VMware Inc. (1999) “VMware Technical White Paper”, Palo Alto – CA - USA.

[10]. Vmware Emulator. http://www.vmware.com.

[11]. https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

[12]. https://www.proofpoint.com/us/threat-reference/email-spoofing

[13]. https://www.educative.io/answers/what-is-a-backdoor-attack

[14]. https://www.javatpoint.com/active-attack-vs-passive-attack