EAI Endorsed Transactions
on Cloud System

Research Article EAI.EU

VIRTUALIZATION TECHNOLOGY – THREAT OR OPPORTUNITY

Wg Cdr N Ramakrishnan[1] ,and Dr. T Subbulakshmi[2]

[1]Research Scholar, SCSE, VIT University Chennai, n.ramakrishnan2015@vit.ac.in
[2]Senior Professor, SCSE, VIT University Chennai, subbulakshmi.t@vit.ac.in

Abstract

The methods used to build the Information Technology (IT) Infrastructure in this modern digital world are radically different and are very new when it's compared to the older methods that were in vogue. One such different methods encouraged by this modern world of cloud services is the use of virtualization technology that support to erect the IT infrastructure. The buzzword 'Virtualization' is not new in this IT field as it was introduced in 1960s by IBM while trying provide solution to accommodate multiple users over expensive computer resources with time shared solutions. This solution supported every technology and protocols of physical computer infrastructure. Even though it kept evolving over the years, the technology achieved its reach with the introduction of VMware workstation by VMware Company in year 1999.At present there are enough solutions available to virtualize our computer resources and services. However the rush seen in embracing this technology has not been justified when we consider the security notion attached to it. Virtualization by itself is not a security solution for our IT infrastructure. In fact it increases the attack surface area, along with the more probability of successful execution of various cyber-attacks. This paper is intended to study in detail about the threats that are to be understood while operating in virtualized environment.

Keywords: Virtualization, Virtual machines, Threats, Virtualization Security.

Received on 08 March 2018, accepted on 03 April 2018, published on 11 April 2018

doi: 10.4108/eai.11-4-2018.154466

1. Introduction

Cost-Effective utilization of IT infrastructure and flexibility in adapting to organizational changes are the top two business challenges for IT managers. Constraints in budget and more regulations adds further difficulties to these challenges. The Technological innovation that allows IT managers to come out with creative solutions to such business challenges is called as "Virtualization". A virtual machine can be defined as a soft machine, like a physical computer, can run its own operating system and other applications. The platform that can consolidate the computing resources and serves it to run more number of machines over the same hardware is called hypervisor. Also virtualization does not only refer to the act of breaking into multiple entities. It can also be used to consider multiple entities into single entity. For example multiple hard disks can be made to be seen as single storage device with the help of virtualized layer. Thus the technology can be conveniently defined as "Abstraction of computer resources". It can be making many virtual resources from single physical resource or consolidating many physical resources into single virtual resource. Conceptually it can be classified into various types namely Server virtualization, Desktop virtualization, Network virtualization, Storage virtualization and Application virtualization. The paper is aimed to concentrate on the types defined with the help of the abstraction layer called as hypervisor [1]. The two important types of this technology Type-I and Type-II will be explained in para 2 and para 3 respectively. Security requirements and benefits are discussed in para 4 followed by security standards in para 5. The threats of virtualized environments are

discussed in paragraphs from 6 - 9. Statistical analysis on the vulnerabilities and exploits present in virtual environment reveals that most of the challenges are towards the security of the hypervisors and is explained in para 12. It needs to be accepted that the technology has opened more vectors for attackers to penetrate into this virtualized environment. Possible solutions to these threats are discussed along with the threats and final recommendations are in para 13.

2. Type-I Virtualization

Separation of a resource or request for a service from the underlying physical delivery of that service can be described as Virtualization. This deployment is non-disruptive, as the user experiences everything the same as the maximum remain unchanged. One of the most famous approach is the Type-I virtualization where a hypervisor is available at boot time of machine in order to control the sharing of system resources across multiple VMs. In a virtualized system, the hypervisor (or virtual machine monitor) application provides an emulated hardware device - a virtual machine (VM)-for each virtual OS[2]. The hypervisor handles each virtual OS's communications with the CPU, storage system, and network. The hypervisor allocates the system resources that each virtual OS needs and ensures that they don't disrupt one another. In essence, it pools hardware resources and allocates them dynamically. Thus the hypervisor forms the nerve center for the VMs. As the hypervisor is directly erected over the bare metal, this type of virtualization is also called as "Bare Metal Virtualization".

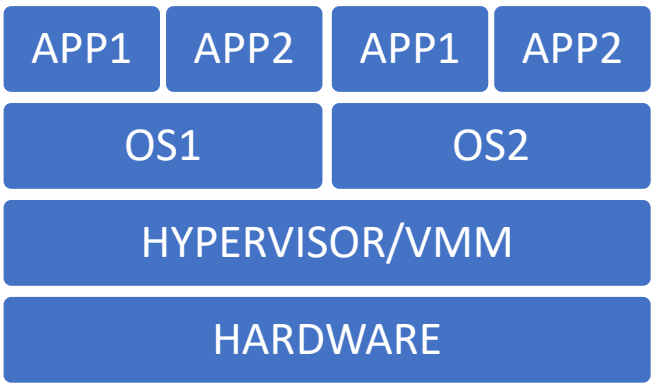


Figure 1. Type-I Virtualization

3. Type-II Virtualization

In Type-II virtualization rather than hypervisor acting directly over the hardware, the host operating system lies in between hypervisor and host hardware [2]. Hypervisor is like another application that runs over the host OS. Virtual machine instances called as guest machines run in respective contained environment above the host OS with the help of hypervisor over the host operating system. The another notable difference in hypervisors present between Type-I and Type-II virtualization is that in Type-I virtualization the hypervisor runs at Kernel ring 0 level whereas in Type-II it runs at ring 3 level. Even though the hypervisor is in ring 3, the kernel of guest OS are given a belief that they are operating in ring 0 of that metal. This helps the user not to appreciate any difference due to the act of virtualization. [3]

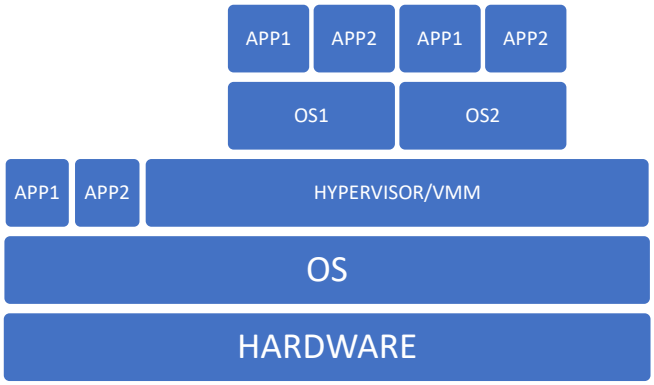


Figure 2. Type-II Virtualization

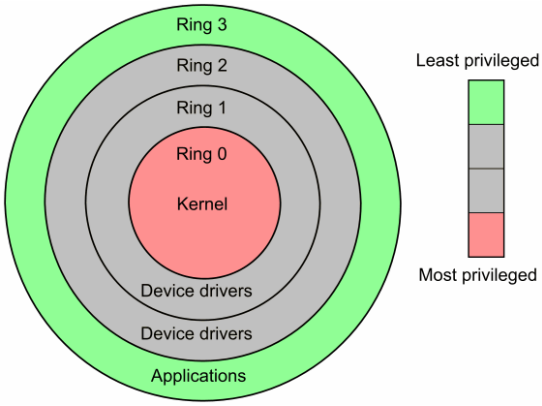


Figure 3. Privilege Ring Levels

4. Security Requirements

Virtualization definitely modifies the relationship between the OS and underlying hardware for computing, storage or even for net-working .In virtual environments client and server class machines are hosted using

hypervisors. Security requirements remains same in virtual environment as the threats which affect information security in a physical world also has the potential to affect virtualized world. In fact it will be more devastating in virtual environment because of the reach they get after penetrating into a virtualized environment, where all virtual instances are within the same physical host. May be this is the reason that few researchers consider the use of virtualization itself as cause that increased the security concern significantly. It is because multiple virtual machines run on the same server, one of them may be malicious VM exampleVM3 in Fig 4 which will get the opportunity to compromise the virtualization layer. Since the virtualization layer plays a major role in the overall operations of virtual machines, a successful attack would give the full control of all VMs to the malicious VM. This potentially compromises the confidentiality and integrity of the software and data of all virtual machines including the host machine.

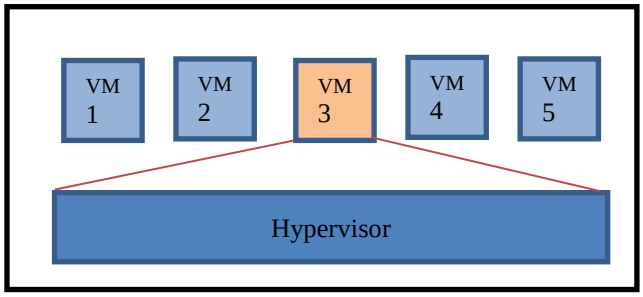


Figure 4. Compromised VM

The traditional security methods like physical security, network security [Firewall], malware [IDS] security etc will be insufficient in securing virtualized set up. The security methods needed for virtual environment are new and more than required than that of traditional security. In spite of additional security measures that are required, it is really worth in making and securing virtual infrastructure as it would be able to provide lots of benefits. Few are listed below.

(i) Virtualization reduces the hardware requirements and improve physical security as there would be fewer devices and data centres to secure.
(ii) "Snapshot" feature in virtualization will help to revert back to safe state existed prior to attack in shortest time.
(iii) Incident handling becomes easy as the services can be restored or replaced in no time with the help of "Snapshot" and "Migration" features.
(iv) With proper isolation between the hosted machines/services, the attack can be contained to one particular application or OS.
(v) Virtual switches inadvertently prevents the network from various network level attacks like DTP Dynamic Trunk Protocol) attack, MITM(Man In The Middle) etc as they don't have the facility to entertain several vulnerable features of physical switch like dynamic trunk protocol, double encapsulation etc.

5. Security Standards

There are various standards that are in vogue to ensure information security of the companies that are in business at present. All these standards are strictly ensured during the audits that can permit their presence in corporate world. Few of those standards are mentioned in following lines. Key privacy and security-related regulations include Payment Card Industry – Data Security Standard (PCI-DSS), for all organization that accepts or processes credit cards; Health Insurance Portability and Accountability Act (HIPAA), for healthcare agencies and for those that handle healthcare records, Gramm-Leach-Bliley Act (GLBA) for financial institutions' collection and disclosure of customer personal data; Family Educational Rights and Privacy Act (FERPA), for public educational institutions' protection and disclosure of student records; Massachusetts "Breach Notification Law" of 2007, for organization that discloses personally identifiable information (PII).

As mentioned by Red Titter [4] none of these regulations and requirements provide prescriptive guidance on virtualization and related security aspects. There are variety of virtualization solutions available in the market by almost all anti-virus companies. There is a need to standardize the virtualization security solutions incorporated by corporate companies as per their business field. For example the company involved in cloud services may adopt a particular security solution and the medical industry company may adopt another security solution while implementing virtualization technology. These standards will act as guidelines for deciding on the security standards that are required in virtual environment.

6. Security Threats

Virtualized environment is also known for the presence of variety of threats. Threats are nothing but the potential danger which is always present in the environment. Even though virtual machines run in separate container over the host operating system, the network requirements make the guest machines to use the same interface. This creates the opportunity for most of the attack vectors function successfully. The authors of "Virtualization security: Analysis and open challenges" [5] explained the different

directions from which a virtual [6] environment can perceive the attack. The paper has also nicely tabulated the attack directions that are possible in this environment(Fig.5).The same are explained pictorially referred vide Fig 6 -11.These threat directions indicate the devices in VM environment that can act as a source for successful execution of respective attacks.

Source	Explanation
NW → VMM	Attack from outside the network to VMM
NW → VM	Attack from outside the network to guest VM
VMM → VM	Threat from VMM attacks to VM
VM → VM	Threat from one VM to another VM
Admin → VMM	Cloud service providor admin threat to VMM
Admin → VM	Cloud service provder admin threat to VM

Figure 5. Threat Directions

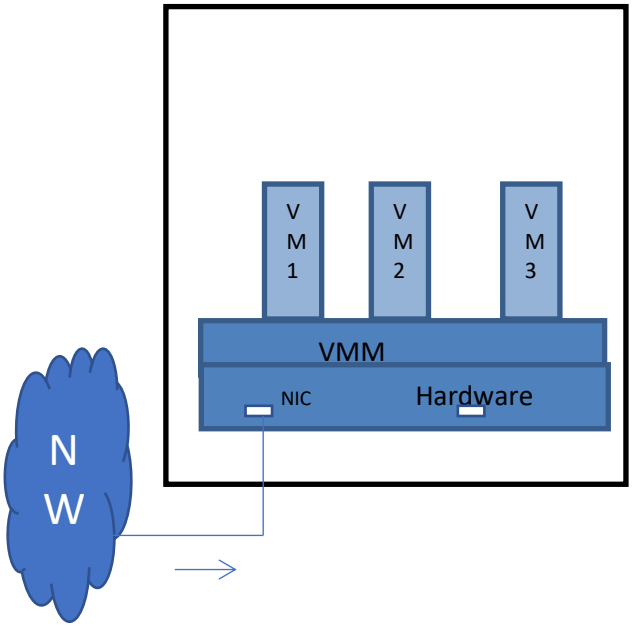


Figure 6. Network to VMM

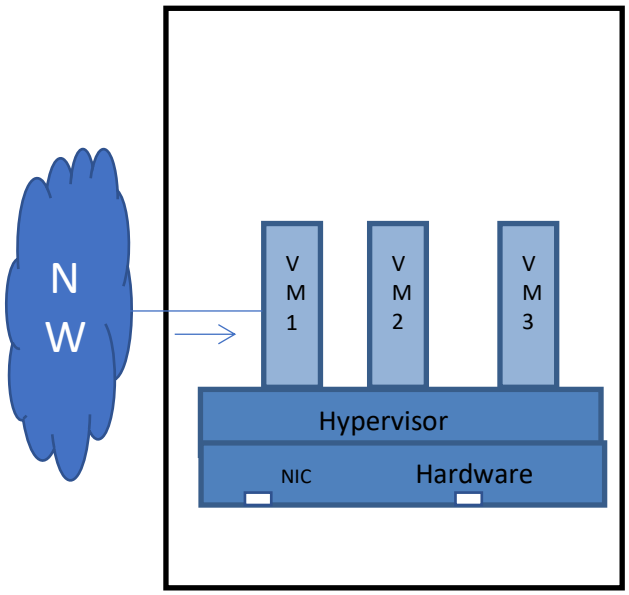


Figure 7. Network to VM

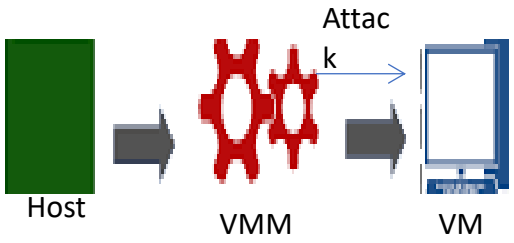


Figure 8. VMM to VM

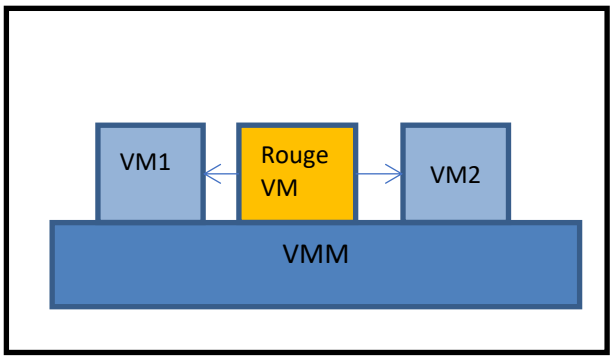


Figure 9. VM to VM

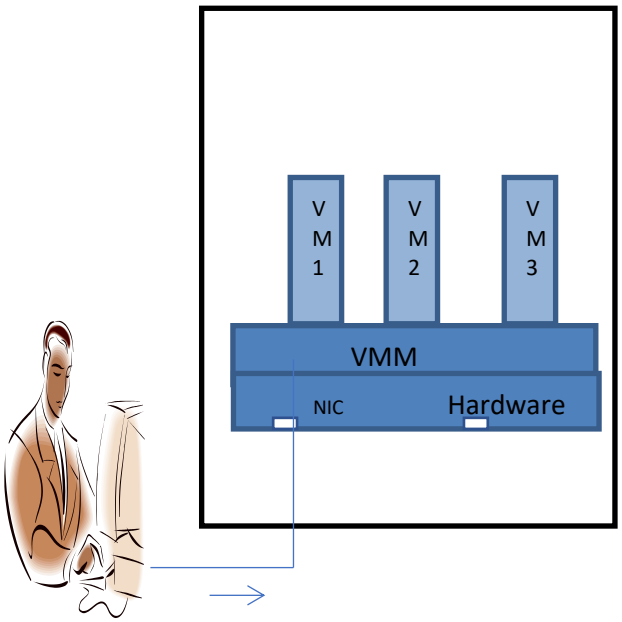


Figure 10. Admin to VMM

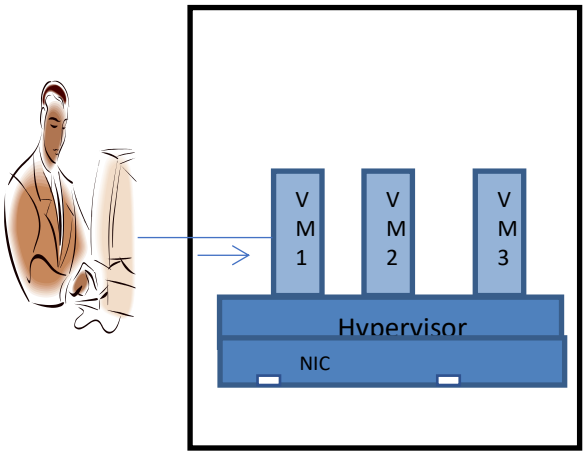


Figure 11. Admin to VM

These possibilities can never be ignored. Ignoring the security needs in configuring controls with virtualization will pose a big problem. At present Software patch updates and vulnerability management controls are mostly limited to individual physical devices. The technicians are also limiting themselves in maintaining physical servers only as it is felt that a separate training and certification is required to operate and maintain virtual servers. Comparatively in the virtualized environment the demands are very high that these configuration management, patch updates, vulnerability assessment and pen testing (VAPT), security audit etc are to be extended to virtual servers. It is actually simple to follow these security procedures in Virtual machine and Virtual networks than on physical devices and networks because of the more centralized controls that can be exercised over virtual networks. Few of the threats are actually escalated to attacks with the help of available exploits and has proved detrimental to the security of IT Infrastructure.

7. Hypervisor Attacks

As we discussed in section II and III, virtualization is managed by one separate layer called as Hypervisors. This layer only enables organizations to run multiple operating systems on a single system and also manages how each of the operating system instances is allocated the resources (processor and memory) it needs to function properly.

Even though this layer should reduce attack probability due to its feature of modular containment, it is proved by facts that the presence of one more layer has increased the surface area of security vulnerabilities which could be leveraged to attack by sophisticated exploits made available by the attackers.

After all configurations the VMM has to be operated in the networked environment that is already existing. The possibilities of network level attacks like ARP poisoning cannot be ruled out by the presence of virtual environment. The vulnerabilities can be from network side or from the weakness like kernel or the add-ons present in the hypervisor. This vulnerability can be exploited to gain control over the VMM and same can be pivoted to control or steal the data flow from the virtual machines that are positioned above the hypervisor. In case of client side attack like any browser exploit then the virtual machine is compromised first and then the same can be escalated to control the hypervisor. As shown in Fig.12, thus there is a bright chance of hypervisor being attacked from both the sides in this virtual environment.

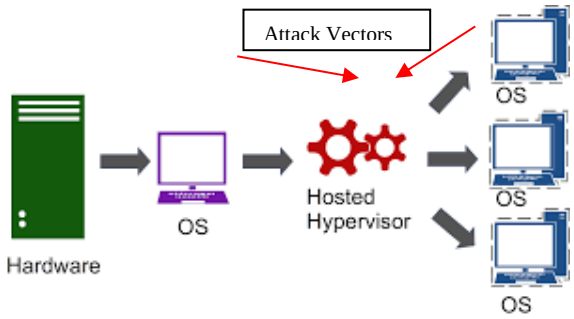


Figure 12. Hypervisor Attack

7.1 Source

It is because of the position of the hypervisor, there is a potential attack possible in two ways, one from the guests running above the layer or from the compromised host running below that hypervisor. When it comes to Type-I virtualization the attack is directly by the firmware itself. This attack of hypervisor from firmware and hardware was explained by the report by Advanced Threat Researchers Mikhail Gorobets & team in the paper presented in DEFCON-2015[19].

It is the default hypervisor behaviour on a network that it responds to connections through standard TCP/IP, something same as that of physical computers and network infrastructures. Thus it is possible to locate the layer on the network and consequently susceptible to traditional network enumeration attacks.

7.2 Attack Methodology

Network enumeration tools like Nessus will be of big help in collecting the details of this layer. The response or the information returned will be used to analyse the layer and extract further information from its characteristics. One such tools can be the enumeration tool Nmap with '–O' switch, which can compare the response of host for a particular packet with the database maintained. With this analysis and information that has been identified, it is possible to interrogate the hosts further to disclose some more details like kernel version, patch details etc. Depending on the applications and the data collected the attacker will be able to find the appropriate CVE (Common Vulnerabilities and Exposures) for which the host may be vulnerable. Depending on the successful exploits available they are graded using the Common Vulnerability Scoring System (CVSS).More the score better the attack possibility and success.

7.3 Known Attacks

With the identified vulnerabilities, it is possible by the attacker to exploit the system and insert a payload to further control the host and maintain access. Some of the famous and reliable tools at present to exploit systems and feed malicious payloads are Metasploit and CORE Impact. Modular design in hypervisors like Xen and KVM enable extensions to their basic functionalities – Hypervisor Add-ons. For example, the National Security Agency (NSA) has their own version of Xen's Security Modules (XSM) called FLASK [16]. In general hypervisor add-ons may increase the vulnerabilities being present in hypervisor, as they increase the size of the Hypervisor's codebase. One such vulnerability is CVE-2008-3687 that describes a heap overflow opportunity in one of Xen's optional security modules, FLASK, which results in an escape from an unprivileged domain directly to the Hypervisor. The unprivileged domain user can execute an arbitrary code using one of the flask hyper call. The CVSS for this is 6.82 and the attack vector for this attack is declared as the network media [17].

7.4 Mitigation

Hypervisor attacks are capable compromising the whole IT infrastructure and they can be mitigated by following actions.

(i) For Type-I setup, simple hardware emulation fuzzing modules can be used to test firmware before installing the hypervisor over it.

(ii) For Type-II setup, the base OS needs to be hardened at all levels to ensure secured hypervisor in the application layer.

(iii) Fuzz all hardware devices before use to identify vulnerabilities in CPU emulation.

(iv) Attack from hosted machines can be mitigated by ensuring strict Access Control List (ACL) that prevent the reach of hypervisor from the attacker.

8. VM Attacks

Virtual Machines are supposed to work in contained environment over the host hardware. However there is a possibility for some process to escape from these containers and provide access to unauthorised users or data. Also the attack on one machine can traverse to another over the same host.

8.1 Source

The main source of this type of attack is the hosted VMs. These rogue VMs are VMs that manage to subvert the access control function provided by the virtual machine monitor/hypervisor to hardware resources such as memory and storage. This is like escaping from the control provided for restricting the virtual machine in a container and have access to host operating system or hypervisor for gaining

resources pertaining to host or other guest machines.

The possible reasons for this threat aremisconfiguration of the hypervisor and/or guest VM container, or malicious or vulnerable device drivers. If a rogue VM takes control of the hypervisor, it will be having the potential to install rootkits or attack other VMs on the same virtualized host. Few of the vulnerabilities that have been demonstrated in this concept of escape are CVE-2009-1244, CVE-2011-1751, CVE-2012-0217 (Xen, 2012), CVE-2012-3288.The implications of escape of a guest, running on an enterprise 'Type 1' hypervisor such as ESXi or the Xen hypervisor would be much greater due to the environments and services that they are often employed in and employed for.

8.2 VENOM

Another recent famous VM escape attack is 'VENOM' [Virtualized Environment Neglected Operations Manipulation] identified by Jason Geffner [7]. The hacker from any guest machine could hijack the data from the memory space of the host operating system by using the perennial buffer overflow vulnerability(CVE-2015-3456) in the floppy disk drive of the quick emulator [QEMU].This is highly possible in QEMU based applications like KVM, Zen and Virtual Box[8]. The reason is that this buggy floppy device controller is loaded automatically in memory even though we don't configure it for any floppy drive device. The steps of this hack are explained with the help of Fig.13.

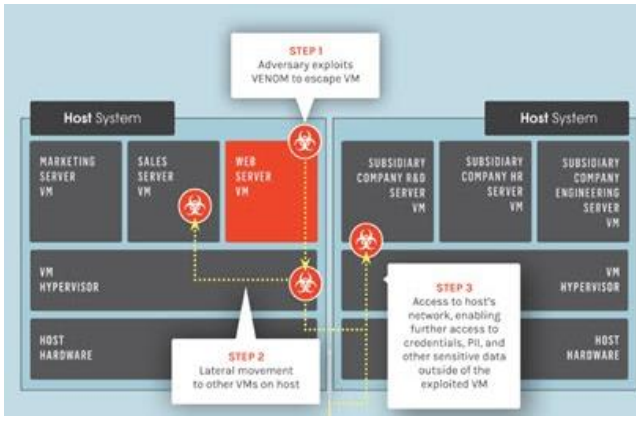


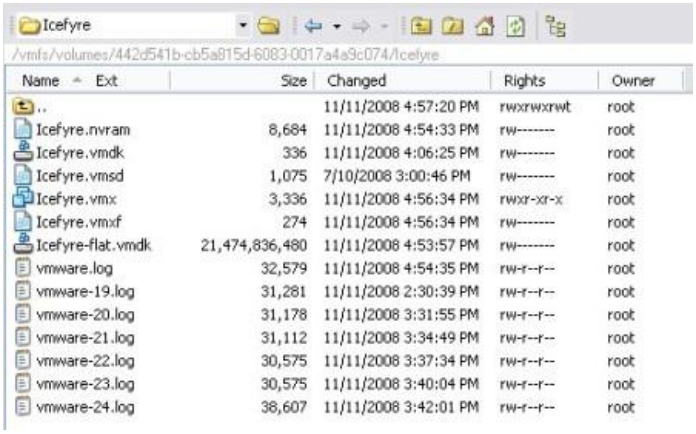
Figure 13. VENOM Attack

8.3 Mitigation

The only thing that can be saving solace from this 'VENOM' attack is that it is mandatory for the attacker to have root privilege for exploiting the buffer over flow vulnerability as mentioned earlier. Servers operating in standard user privilege mode will not be effected by this 'VENOM' attack.

9. Cache Attack

VMFS. Virtual Machine File System (VMFS) is the technique used by VM Ware to manage the file system of the virtual machines that are made over the hypervisor or VMM[9][10]. One look at the files that are associated with the guest machine will indicate that most of the files start with the actual name of the guest machine followed by different file extensions that denote the file type [11][12][13].It is not possible to see all of the possible file types in the VMFS until our VM is in a certain state. For example, the .vswp file can be sighted only when the VM is powered on and the .vmss file makes its presence only when a VM is suspended. The .vmx file holds all of the configuration information and hardware settings of the guest machine. All of the information related to settings that are edited in the virtual machine are stored in text format in this file. This file store a wide variety of information about the VM, including its specific hardware configuration like RAM size, nic information, hard drive information and serial/parallel port info advanced power and resource settings, VMware tools options, and power management options etc. It is possible to edit this file directly to make changes to a VM's configuration.


Icefyre

/vmfs/volumes/442d541b-cb5a815d-6083-0017a4a9c074/Icefyre

Name	Ext	Size	Changed	Rights	Owner
..			11/11/2008 4:57:20 PM	rwxrwxrwt	root
Icefyre.nvram		8,684	11/11/2008 4:54:33 PM	rw-------	root
Icefyre.vmdk		336	11/11/2008 4:06:25 PM	rw-------	root
Icefyre.vmsd		1,075	7/10/2008 3:00:46 PM	rw-------	root
Icefyre.vmx		3,336	11/11/2008 4:56:34 PM	rwxr-xr-x	root
Icefyre.vmxf		274	11/11/2008 4:56:34 PM	rw-------	root
Icefyre-flat.vmdk		21,474,836,480	11/11/2008 4:53:57 PM	rw-------	root
vmware.log		32,579	11/11/2008 4:54:35 PM	rw-r--r--	root
vmware-19.log		31,281	11/11/2008 2:30:39 PM	rw-r--r--	root
vmware-20.log		31,178	11/11/2008 3:31:55 PM	rw-r--r--	root
vmware-21.log		31,112	11/11/2008 3:34:49 PM	rw-r--r--	root
vmware-22.log		30,575	11/11/2008 3:37:34 PM	rw-r--r--	root
vmware-23.log		30,575	11/11/2008 3:40:04 PM	rw-r--r--	root
vmware-24.log		38,607	11/11/2008 3:42:01 PM	rw-r--r--	root

Figure 14. VMFS Directory

9.1 Side Channel Attacks

Thus it is clear that all data of the guest machine is stored as file in the host memory. This gives the possibility for the attacker to steal these files or spoil the integrity of these files. One such attack is cache timing attack that exploits the cache architecture of modern CPUs. These are also called as side channel attacks in which the cloud data are stolen by using this file cache. The cache memory details are reused to hack into the application without the user knowledge and the same can be demonstrated by simple application like Gmail.

In following figure 15 the Gmail application is opened using the password by the genuine user and while using it the application used for erecting the virtual machine was closed without carrying out the shutdown of logged in VM. The user also did not log out from the Gmail application that was under use. After five minutes 12:23 PM the application was started again to fire up the ubuntu virtual machine that was in use before closing. After the machine was fired up , the Gmail application could also be opened directly with the cache details present in the file system without any need for the user to log in again into the Gmail (Fig 16). It is evident that the RAM details including the password was stored in the virtual machine file system and same was used on machine start up. The same details could be analyzed for the extraction of credentials from the file storing RAM details.

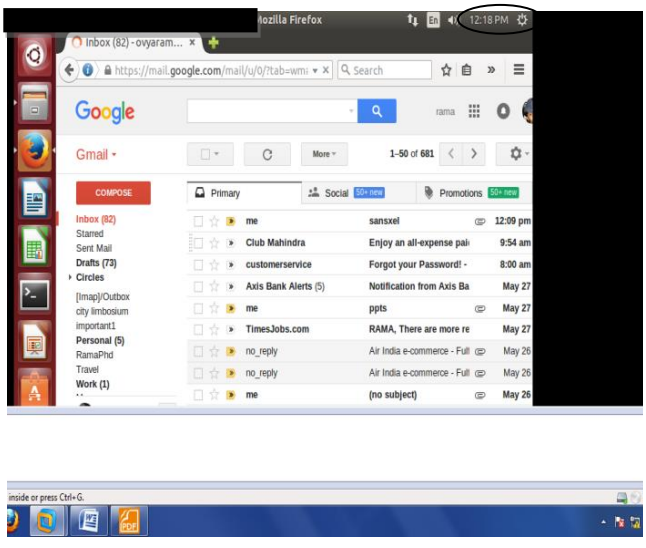


Figure 15. Gmail App

The reason for successful entry into the e-mail application is that the RAM dump of these virtual machine are stored as files in host machine. The security issue is that these files are stored in user accessible directory and are neither encrypted nor hidden. This makes it possible for the attacker to access these files and steal or manipulate data. RAM details that are stored in binary format in .vmbin file cane be analyzed by the use of tools like 'Hexplorer' for credential extraction.

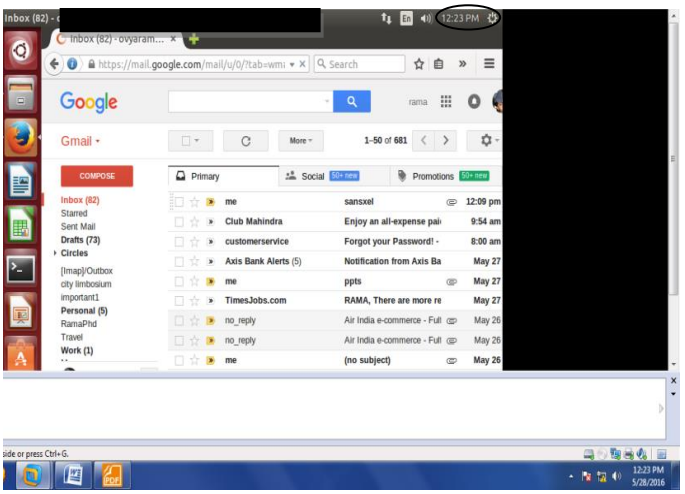


Figure 16. Cache Attack

9.2 Mitigation

(i) The files pertaining to guest machines that are stored in host machines are to be encrypted.
(ii) The memory disk used for hosting guest machines are to be mounted by authorised users only.
(iii) Ensure proper shut down of the VMs before closing down.
(iv) Restrict write permissions by unauthorised users to the files that are stored in local host.

10. Resource Starvation

Server utilization can be dramatically increased by means of running several virtual servers over the same metal in place of having separate hardware for separate services. But this can also pose the threat of increasing the burden on hardware resources. For example, the issues with input

output can occur when multiple VMs on a single server share the same network card (Fig.8). That too these type of threats are very high especially in I/O-intensive applications. Most of the applications are made to optimize their I/O operations for specific hardware platforms, in a Virtualized environment and those optimizations are at times lost in the hypervisor translation layer.

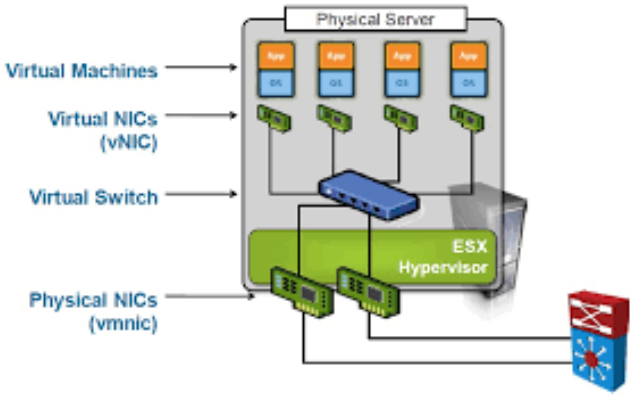


Figure 17. Multiple VMs

If this optimization is not ensured then this can be a major factor that can degrade network performance and also assist in increased response-time latency. For example, a virtual serverhosting an I/O-intensive application may have to process hundreds of SSLencrypted sessions, which will be highly demanding on the host metal.

Physical memory resource crunch is also experienced while virtual servers carryout deep scanning activities. For example the remote control process of Micro Soft SCCM server named CmRcService.exe starts with 1.3GB then jumps to 2.5GB of virtual memory utilization. In this condition there is a possibility that the Server runs may out of RAM and get itself locked up till the scan scan completes successfully. During this brief period it needs to be accepted that there will be business outage. Attackers are interested in creating such more situations so that the business is at risk. Variety of memory handling techniques are available to mitigate such risks.

Virtualization administrators concentrate on the configuration of High Availability to protect the performance of virtualized applications that has toequate the business value. That means when you assign more resource to less number of virtual machines then it is wasteful, while assigning too lesswill starve a VM, Which results in poor performance in virtualized environment. An attacker is more interested in creating this situation in which he will succeed in making the guest machines to starve for resources by misconfiguring or originating simple attacks. Misconfigured or malicious VMs may be consuming a disproportionately high percentage of host resources, resulting in other VMs being denied (starved of) service.High CPU utilization on host will make the other servers to starve of process cycle.Attacker intend to initiate multiple special Processes that consume a substantial amount of resources to prevent correct operation.

10.1 Mitigation

Memory managing techniques varies for an actual machine and a virtual machine which is operating over the hypervisor. The basic four methods that are followed by virtual machines for managing the physical memory under hypervisor are listed below.

- Memory compression
- Ballooning
- Transparent Page Sharing
- Paging

Understanding memory managing techniques by virtual machines and hypervisors explained by VMware need to be understood for handling such situations [18].

11. Malware Attack

Virtualization technology has been adopted by 70% and more organizations till year 2015 for providing virtual servers and desktops.Malware analysis has been carried out for a long time in virtual machines due to the isolation and contained environment provided by this technology. This has led to the misconception that the malware disappears once it identifies the machine has a virtual machine. But the fact is in present date there are malware that look for virtual servers mainly as new tactics to infect virtual machines in our environments. One such example is “Crisis Malware” [14] which can actively seek for VMware virtual machine files. Once the machine is compromised, Crisis mounts the disk and then make use of native VMware facility and then insert into the disk file to infect the virtual machine.File infection can be applied to entire file system and malware keeps spreading on all files. Most of the malware that are well known have the capability to detect this virtualization technology. Conficker worm (year 2007 & 2008),

Storm worm (year 2008 & 2009) are few of the malware that proved of having VM detection routines. With the adoption of virtualization more in recent past, it is true that server-oriented malware are highly prevalent to infect virtual servers than physical servers in many organizations. These malware will wait for few number of random clicks to begin their malicious activity which makes it harder to detect in automated virtual environments.

12. Statistical Analysis

Statistics on the vulnerability identified in virtualization environment can be obtained from the details provided by national vulnerability database (NVD).NVD is the central repository that manages data on vulnerabilities identified all over the world. This database is managed and maintained by US. Government agencies. Authors of "Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers" analysed all of KVM's and Xen's CVE reports from the vulnerability databases, labeling each with its functionality-based attack vector [15]. Following the similar lines the data was searched for both kvm and xen type of packages as on date. The details are tabulated below.

Table 1. Attack Statistics

SlNo	Target	Xen	KVM	Total
1	Hypervisor	31	18	49
2	Host OS	41	33	74
3	Guest VM	4	1	5

These identified vulnerabilities can be further classified in to low, medium, high and critical risk category depending on their values in Common Vulnerability Scoring System (CVSS). The item wise threats can be divided between these risk categories that are listed below.

- "Low" risk if CVSS = 0.0-3.9.
- "Medium" risk if CVSS = 4.0-6.9.
- "High" risk if CVSS = 7.0-8.9.
- "Critical" risk if CVSS = 9.0-10.0.

A total of 49 serious vulnerabilities and available exploits indicate the importance of securing hypervisor as it is targeted to ensure deep impact and scale in large scale.

13. Recommendation

With this technology multiple operating systems or multiple sessions of a single OS can be run on a single PC or server. This helps the organizations to use their hardware more efficiently. Similarly, it is possible to apply virtualization techniques to other IT infrastructure layers like networks, storage, server hardware, operating systems and applications. This paves way for different types of virtualization like memory virtualization, network virtualization, I/O virtualization etc. The security requirements and solutions for each type of virtualization will be different. It is much more difficult to address security issues post deployment and implementation due to this diversity. There are lot of Anti-Virus companies providing solutions for the virtual environment made using RHEL or VMware products. It is recommended to follow.

(i) Initial planning stage should consider all security requirements.

(ii) The security design must be in place for providing the solutions as per the planned infra-structure.

(iii) The frame work for security design should include all layers of security and all aspects of CIA triangle.

(iv) Tailor made security frame works are to be designed and assessed for its vulnerable free operations.

(v) Pentest needs to be satisfied before considering implementation of any such frameworks or models.

14. Conclusion

Now a days it is more economical to erect servers in virtualized environment rather than real physical servers. The very first step in securing these servers is to secure the underlying hypervisor and operating system. Standard procedure for Server hardening is to be elaborated in security policy itself. Configuration and tuning of servers are to be strictly based on these policies only Implementation of cloud services and ensuring its security are totally different from traditional grid computing. It is therefore obvious that so many researchers are in the process of providing information security solutions. Most of the security related researches are limited to proposing a novel architecture or model which has its own practical

implications. Few companies claim the availability of commercial solutions for virtual infrastructure which are very costly and beyond reach of normal users. Researchers have a big scope in these areas where there is a need to find economic workable solutions for virtual environment.

References

[1] VMware, Inc, "Virtualization overview "[Online]: https://www.vmware.com/pdf/virtualization.pdf

[2] Scott Delap, "Virtualization Intro" [Online]: https://www.infoq.com/articles/virtualization-intro

[3] Dave Shackleford, "Virtualization Security: Protecting virtualized Environments " : Book published by Jhon Wiley & Sons. ISBN: 978-1-118-28812-2

[4] Ted Ritter, "Virtualization Security
Achieving Compliance for the Virtual Infrastructure"
Senior Research Analyst, Nemertes Research [Online] http://la.trendmicro.com/media/wp/virtualization-security-nemertes-whitepaper-en.pdf

[5]Muhammad Arif and Haroon Shakeel, "Virtualization security: Analysis and open challenges", Faculty of Computer Science and Information Technology, University of Malaya 50603 Kuala Lumpur, Malaysia, Computer Science Department, Comsats Institute of Information and Technology Islamabad Pakistan, International Journal of Law and Information Technology February 2015

[6] Gabriel Cephas Obasuyi, Arif Sari, "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment", Management Centre of the Mediterranean, Nicosia, Cyprus, Int. J. Communications, Network and System Sciences, 2015, 8, 260-273

[7] https://johncouzins.wordpress.com/2013/11/27/attacking-the-hypervisor/

[8] Jason Geffner, "VENOM" CrowdStrike Senior Security Researcher, [Online]:http://venom.crowdstrike.com

[9] Brian Donohue,"All you need to know about VENOM virtualization vulnerability", [Online]: https://blog.kaspersky.com/venom-virtualization-vulnerability/8743/

[10] VMware, Inc, "VMware® vStorage Virtual Machine File System" [Online]:https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-vmfs-tech-overview-white-paper.pdf

[11] Michael Principato, "Virtualization technology and Process Control System upgrades", Heidelberg Technology Center - HeidelbergCement, Allentown/Leimen, Germany Technical Conference, 2010 IEEE-IAS/PCA 52nd

[12] Satyam B.Vaghani "Virtual Machine File System" VMware, Inc [Online]:https://www.researchgate.net/publication/220623259_Virtual_machine_file_system

[13]VMware, Inc, VMFS, [Online:] https://www.vmware.com/support/ws55/doc/ws_learning_files_in_a_vm.html

[14]VMware, Inc, VMFS Best Practices, [Online:] http://www.vmware.com/pdf/vmfs-best-practices-wp.pdf

[15] Kaspersky, "Malware analysis:How some strains'adapt' to virtual Machines" [Online]: http://www.bitpipe.com/detail/RES/1477288811_51.html

[16] Diego Perez-Botero, Jakub Szefer and Ruby B. Lee, "Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers,"in Proceedings of the Workshop on Security in Cloud Computing (SCC), May 2013.

[17] SUSE security updates [Online]: https://www.suse.com/security/cve/CVE-2008-3687/

[18] Understanding Memory Resource Management [online]: http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/perf-vsphere-memory_management.pdf

[19] Mikhail Gorobets & team, Attacking Hypervisor Via Firmware [Online]http://www.intelsecurity.com/advanced-threat-research/content/AttackingHypervisorViaFirmware_bhusa15_dc23.pdf