International Journal of Engineering & Technology, 7 (4) (2018) 5449-5455

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.25161
Research paper

Advanced Security Threats and Mitigation Techniques in Virtualized Environment

N.Ramakrishnan[1]*, Dr.Subbulakshmi.T[2]

[1]Research scholar, School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India
[2]Professor, School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India
**Corresponding author E-mail:n.ramakrishnan2015@vit.ac.in*

Abstract

‘Virtualization’ is not the new buzzword in IT field as it was introduced in 1960s by IBM while trying providing 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.However the rush seen in embracing this technology has not been justified when we consider the security issues attached to it. Virtualization by itself is considered erroneously as a security solution. 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 advanced threats and their mitigation techniques that are to be understood while operating in virtualized environment.

Keywords:*Virtualization; Virtual Machines; Threats; Mitigation; Virtualization Security.*

1. Introduction

The methods used to build the Information Technology (IT) Infrastructure in this modern digital world are radically different and very new when it’s compared to the older methods that were in vogue. One such different method encouraged by this modern world of cloud is the use of virtualization technology that supports to erect the IT infrastructure. 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 add further difficulties to these challenges. This is a Technological innovation that allows IT managers to come out with creative solutions to such business challenges. A virtual machine can be defined as a soft machine, similar to a physical computer that can run its own operating system and other applications. The software or firmware stack that can consolidate the computing resources and serves it to run more number of machines over the same hardware is called hypervisor. Virtualization does not only refer to the act of dividing resources for the use of multiple entities. It can also be used to consolidate multiple resources into single entity for use. 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, Application virtualization etc. 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 next section. Security requirements and benefits are discussed in section III followed by security standards in section IV. The threats of virtualized environments are discussed in sections from V - X. 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 section XI. 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 section XII.

2. Types of 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 functions as 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".

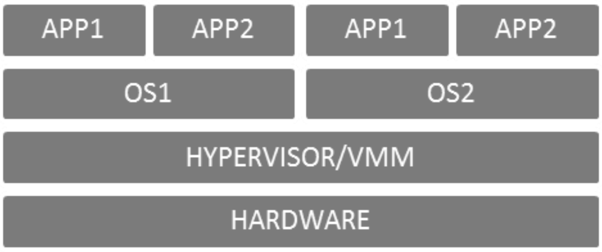

Fig.1 Type-I Virtualization

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][20]

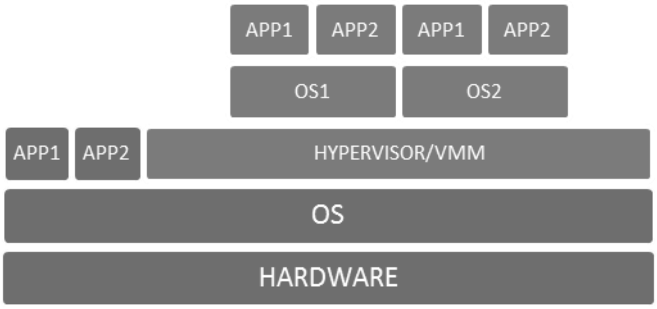

Fig.2 Type-II Virtualization

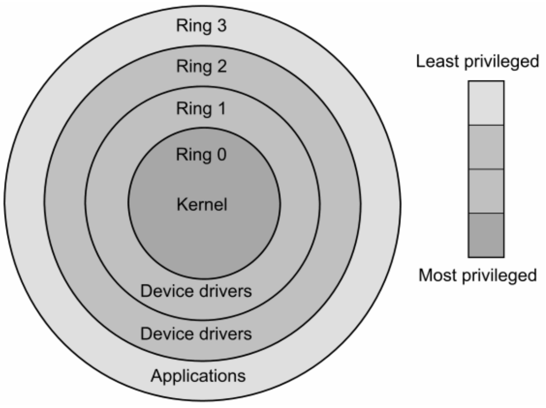

Fig.3. Privilege ring Levels

3. Security requirements and benefits

Virtualization definitely modifies the relationship between the OS and underlying hardware for computing, storage or even for networking .In virtual environments client and server class machines are hosted using hypervisors. Security requirements remain same in virtual environment as the threats which affect information security in a physical world also have 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[21]. 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.

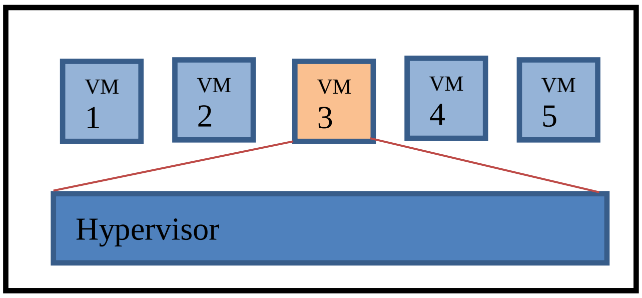

Fig.4 Compromised VM

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 to be novel 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.

a) Virtualization reduces the hardware requirements and improves physical security as there would be fewer devices and data centers to secure.
b) "Snapshot" feature in virtualization will help to revert back to previous state existed prior to attack in shortest time.
c) Incident response becomes easy as the services can be restored or replaced in no time with the help of "Snapshot" and "Migration" features.
d) With proper isolation between the hosted machines/services, the attack can be contained to one particular application or OS.
e) 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.

4. 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 provides prescriptive guidance on virtualization and related security aspects. There are varieties 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 web services may adopt a particular security solution and the big data industry 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. There is a need to fix and achieve required security standards while operating in virtualized environment. Service providers should ensure certain policies like ensuring live migration while providing online web services. Automated backup and log analysis must be insisted in routine. This will not only improve the security standards but also help to make the standard operating procedure that can be easily followed by respective companies for being in the respective businesses.

5. Security threats

In addition to the variety of services and features offered, 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

Table.1 Threat Directions

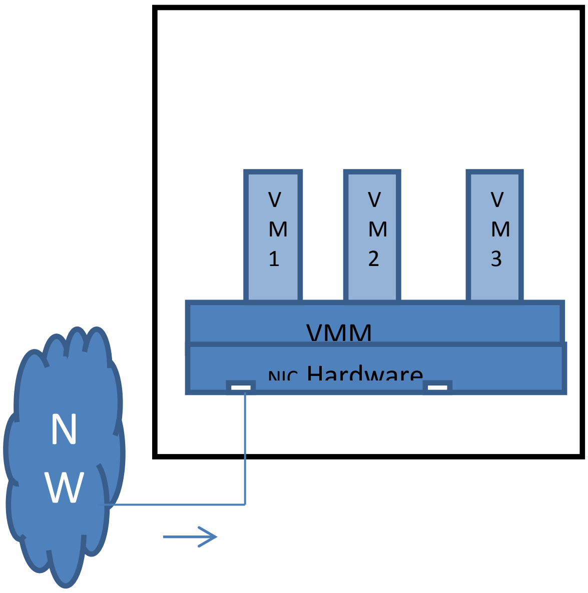

Fig.6 Network to VMM

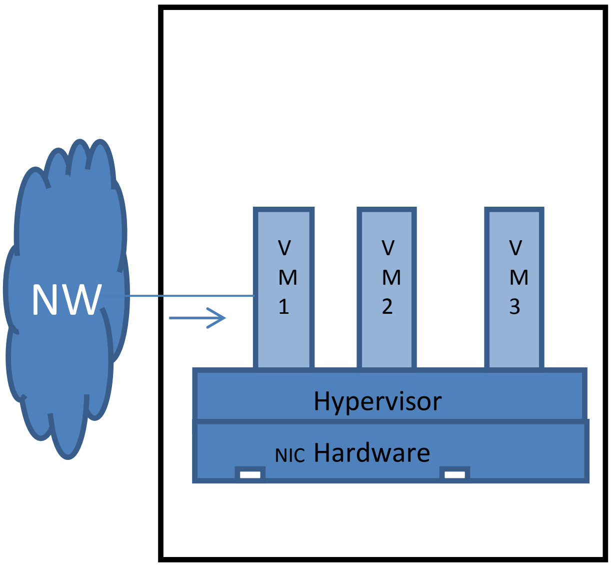

Fig.7 Network to VM

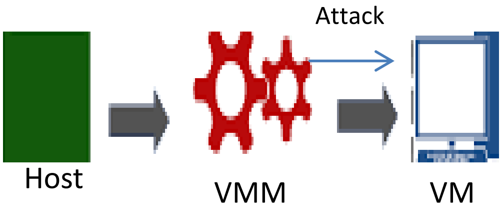

Fig.8 VMM to VM

The directions help in identifying the mitigation procedures that can be adhered for restricting the exploitation. These possibilities for neutralizing the attacks can never be ignored. Ignoring the security needs in configuring controls with virtualization will pose a big problem in production phase. 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 have proved detrimental to the security of IT Infrastructure.

6. Hypervisor attack

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 already exists. 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.9, thus there is a bright chance of hypervisor being attacked from both the sides in this virtual environment.

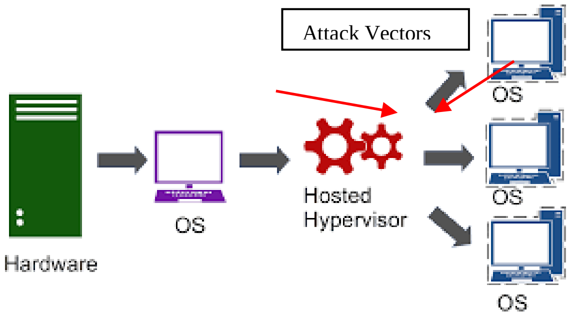

Fig.9 Hypervisor Attack

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 behavior 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.

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 analyze the layer and extract further information from its characteristics. One such tool 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.

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].

Mitigation.

a) For Type-I setup, simple hardware emulation fuzzing modules can be used to test firmware before installing the hypervisor over it. Hypervisor based attestation can be effective to verify the VMs and the applications that were launched[23].
b) For Type-II setup, the base OS needs to be hardened at all levels to ensure secured hypervisor in the application layer.
c) Fuzz all hardware devices before use to identify vulnerabilities in CPU emulation.
d) Attack from hosted machines can be mitigated by ensuring strict Access Control List (ACL) that prevent the reach of hypervisor from the attacker.

7. VM escape

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 has access to host operating system or hypervisor for gaining resources pertaining to host or other guest machines.

Attack Methodology. The possible reasons for this threat are misconfiguration 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.

Known Attacks. A 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. This is the classic example where the administrator is at fault while configuring the peripheral devices for the virtual machine.

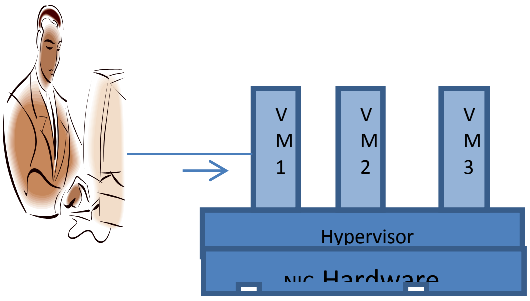

Fig.10 Admin to VM

The steps of this hack are explained with the help of Fig.13.

Step1: VENOM is exploited to do VM escape

Step2: Access other VMs on same host laterally

Step3: Scan the host's network to gain further access to sensitive data like credentials, PII etc.

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 affected by this 'VENOM' attack.

8. 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.

Sl.No	File	Rights	Owner
1	.nvram	rw-------	root
2	.vmdk	rw-------	root
3	.vmsd	rw-------	root
4	.vmx	rwxr-xr-x	root
5	.log	rw-r--r--	root

Table 2. VMFS directory

Attack Methodology. 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 was demonstrated by simple application like Gmail.

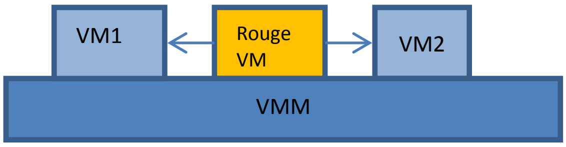

Fig.9 VM to VM

Known Attack. Gmail application remained opened and logged in state while the virtual machine was closed improperly. 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. It is evident that the RAM details including the password were 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.

The reason for successful entry into the e-mail application is that the RAM dumps of virtual machines 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.

Mitigation.

a) The files pertaining to guest machines that are stored in local host memory are to be encrypted to prevent access by attackers.

b) The memory disk used for hosting guest machines is to be mounted by authorized users only.

c) Ensure proper shut down of the VMs before closing down.

d) Restrict write permissions by unauthorized users to the files that are stored in local host.

9. Resource starvation

Multiple VMs or applications run over a single hardware. Any failure in hardware or by the administrator can lead to resource starvation. This phenomenon is generally encountered on unplanned restarts of either application of VMs. 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.

Attack Methodology. Consider the input output issues that can occur when multiple VMs on a single server share the same network card (Fig.8). That too these types 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.

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 server hosting an I/O-intensive application may have to process hundreds of SSL encrypted 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 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. Varieties 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 to equate the business value. That means when you assign more resource to less number of virtual machines then it is wasteful, while assigning too less will starve a VM, Which results in poor performance in virtualized environment [22]. 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 intends to initiate multiple special Processes that consume a substantial amount of resources to prevent correct operation.

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.

a) Memory compression
b) Ballooning
c) Transparent Page Sharing
d) Paging

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

10. 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.

Attack Methodology. One such example is “Crisis Malware” [15] which can actively seek for VMware virtual machine files. Once the machine is compromised, Crisis mounts the disk and then makes 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 numbers of random clicks to begin their malicious activity which makes it harder to detect in automated virtual environments.

Mitigation. Host based IPS or antivirus will be of big help in providing end point security. An un patched computer system becomes easy prey to any malware. It is prudent to ensure thorough patch management process. Windows auto run and drive sharing feature should be disabled to prevent any expansion of such malware. White listed media devices are only be permitted.

11. 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” analyzed all of KVM’s and Xen’s CVE reports from the vulnerability databases, labeling each with its functionality-based attack vector [16]. Following the similar lines the data was searched for both kvm and xen type of packages as on date. The details are tabulated below.

Sl.No	Target	Xen	KVM	Total
1	Hypervisor	31	18	49
2	Host OS	41	33	74
3	Guest VM	4	1	5

Table 3. Attack Statistics

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.

a) "Low" risk if CVSS = 0.0-3.9.
b) "Medium" risk if CVSS = 4.0-6.9.
c) "High" risk if CVSS = 7.0-8.9.
d) "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.

12. 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 lots of Anti-Virus companies providing solutions for the virtual environment made using RHEL or VMware products. Hence it is recommended to have a detailed security plan for implementation[24]. Few of them are listed below.

a) Initial planning stage should consider both perimeter and end point security solutions.
b) Network monitoring must be ensured by automated tools like 'SPLUNK' where the traffic in real time and also the device logs are analyzed for threat detection.
c) The security appliance like firewall or IDPS must be shortlisted in consonance to IT infrastructure.
d) Server hardening procedure like configuring Access Control List, Identity Management, password policy, Remote log collection, Disable unwanted services and network connections etc must be carried out.
e) The security standard planned during set up must be achieved and same needs to be certified by external audit agency. Also the IT audit along with VAPT must be done at regular intervals.
f) Activities like patch management and log analysis are to be meticulously carried out and well documented.
g) Software vulnerability assessment needs to be conducted before hosting any application in the present configura tion.

13. Conclusion

At present 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 https://doi.org/10.1109/CITCON.2010.5469770.

[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.

[20] Piotr Gaj, Mirosław Skrzewski, Jacek Stój, Jarosław Flak, “Virtualization as a way to PC based functionalities” https://doi.org/10.1109/TII.2014.2360499.

[21] Te-Shun Chou, “Security Threats On Cloud Computing Vulnerabilities”, IJCSIT Vol 5, No 3, June 2013.

[22] Arif Khan, “Virtual machine security”, *Int. J. Information and Computer Security, Vol. 9, Nos. 1/2, 2017.*

[23] Hagen Lauer, Nicolai Kuntze, “Hypervisor-based Attestation of Virtual Environments” IEE Journal : DOI 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.125

[24] Leonardo Richter Bays, Rodrigo Ruas Oliveira, Marinho PillaBarcellos, Luciano Paschoal Gaspary and Edmundo Roberto Mauro Madeira, “Virtualnetworksecurity:threats, countermeasures, and challenges”, Springer: Journal of Internet Services and Applications, DOI10.1186/s13174-014-0015-z

[25] Di Lu, Jianfeng Ma, Cong Sun, Qixuan Wu, Zhaochang Sun, Ning Xi,”Building a Secure Scheme for a Trusted Hardware Sharing Environment”, IEE Journal : DOI 10.1109/ ACCESS.2017.2703124, IEEE Access, Vol. 14, No. 8, Aug 2015