Vulnerability Assessment and Penetration Testing of Virtualization

Ramin Vakili [1] and Hamid Reza Hamidi [2]
[1,2]CERT Laboratory, Faculty of Engineering,
Imam-Khomeini International University, Qazvin, Iran
ramin.vakili@edu.ikiu.ac.ir, hamidreza.hamidi@eng.ikiu.ac.ir

***Abstract* - Virtualization brings us lots of significant usages and is a useful technology in data centres and cloud computing. Using virtualization could either reduce security issues or bring new ones. In this research we have tried to review security advantages and disadvantages of virtualization technology. Security specialists assess the security of a system using automatic tools for penetration testing and vulnerability assessment. In this paper, we also review some of the tools that can be used in security assessment of virtualization.**

KEYWORDS - Virtualization, Cloud Computing, Penetration Testing, Vulnerability Assessment

I. INTRODUCTION

Virtualization is a platform which allows us to partition the computer system resources into multiple execution environments. Virtualization increases the utilization of systems and makes the managing of organizations infrastructure easier. This is one of the main reasons that has increased its popularity. Using virtualization would bring some security benefits and it also might cause new security issues [1].

Penetration testing and vulnerability assessment are a set of practical methods which is done by security specialist using tools to assess the security of systems. The goal of these methods is to find the vulnerable parts of a system and to confirm whether the current security measures are effective or not [2]. In this paper we first look at some benefits of security in virtualization and review the main security issues and what causes them. Then we introduce some security tools in the area of virtualization.

II. VIRTUALIZATION SECURITY BENEFITS

One of the main features of virtualization is the isolation between Virtual Machines and their execution environments. This feature makes it possible to have multiple guest operating systems in one host machine and each operating system (OS) runs its own programs in an isolated environment, thus the weaknesses of the programs in one guest OS will not harm the others. Virtualization also has capabilities of recovering the systems to a normal state after any attacks.

The followings are some of virtualization security advantages [3][4]:

- **Better and faster recovery after attacks**

In case of attacks a compromised machine can be immediately restored to a good snapshot which this process is faster and easier than a physical server. Furthermore a copy of a compromised machine can be cloned for later analysis [4].

- **Patching safer and more effective**

Virtualization makes it possible to revert to a previous state if a patch is unsuccessful, making it more likely to install security patches. You can also make a clone of a running server and test the security patches on it [4].

- **Cost effective security devices**

Some security mechanisms and tools like intrusion detection and prevention systems and other security related appliance can be used more cost effective, because we can put them into a Virtual Machine (VM) instead of a physical server [4].

- **External monitoring**

Since VMs run on shared hardware resources, it allows detecting malicious activities and programs outside the VM, unlike the physical installation of OS on a host, which requires an antivirus. The

Hypervisor can monitor VMs and detects anomalies [5].

- **A safe place for testing malware**

A virtual machine can be suitable environment to test and evaluate malwares. Since VMs can be easily cloned, we can merely get a copy of a VM and test the malware. Although there are some malwares that are able to hide and disable some of their functionalities when they run on a virtual environment [5].

III. VIRTUALIZATION SECURITY CHALLENGES

We divide virtualization security issues into four categories, based on where does that particular vulnerability originate. Whether that vulnerability is from guest VM, host machine and VM Monitor (VMM) the security issues is an attack from outside of the virtualization environment or basically the challenge is a management problem [6].

A. Guest VM Security Challenges

In a virtualized environment multiple guest VMs can reside in a single host machine. Thus, these VMs actually run on a shared physical system, which causes some issues. The followings are security vulnerabilities related to the guest machine.

- **VM Hopping**

It happens when an attacker from one guest virtual machine gains access to another virtual machine within the same virtualized environment. Typically, after a successful attack, the attacker is able to monitor the resource usage info, modify configuration, delete data and cause confidentiality issues. Upon this attack happens, the Confidentiality, Integrity and Availability triangle is violated. Since in this scenario, the attacker migrate from one guest VM to another, it is also called guest-to-guest or cross-VM attack [6].

- **VM Escape**

All the allocations of the resources and system assets is monitored by VMM. In other word, guest VMs are never allowed to access the host machine without VMM interfering them. But some flaws and weaknesses may cause a guest OS pass the VMM layer and access to the host machine [1].

If the attacker gains access to the host, consequently he has access to all the host resources including all other guest VMs. There are some types of VM Escape attacks like path traversal which uses command line syntax. VM-chat, VM-cat, VM-ftp and VM Drag-N-Sploit are some tools for communicating between the guest VM and host machine. These tool prove that the isolation between VMs can be violated in some situations [7].

- **Side Channel Attacks**

In side channel attacks, the physical characteristics of hardware like CPU, memory usage and other resources are exploited by the attacker. Because VMs in a virtual environment run on the same hardware, this attack is possible among VMs with shared hardware. These type of attacks requires direct access to the host, therefore they are hard to implement [1]. There are several types of side channel attacks in virtualization like timing attacks, power and electromagnetic analysis attacks, and fault induction attacks. [8].

- **VM Alteration**

Applications that run on a VM depend on infrastructure of virtual machine environment. Therefore these VMs which are running on applications must be trusted and any alteration on the VM will be a threat for the applications [1]. One way to protect VMs against this threat is using digital signature for validating virtual machine files. The signing key should never be placed anywhere it can be compromised and after making any external patches the VM should be resigned [9].

- **VM System Restore**

In the case of attacks or system crashes, system administrators usually restore the VM to the last good configuration. Due to simplicity and quickness, administrators prefer to roll back the system instead of installing new software. But rolling back may cause some security problems and make the system vulnerable. It may re-enable previous users and passwords or reveal the ciphers that were used for data encryption [6].

B. Host Machine or VMM Security Challenges

The followings are security vulnerabilities in the machine that is hosting the virtualized environment can be threatening for all the VMs running on the host machine.

- **Hypervisor Hyper-jacking**

Hypervisor poses some priorities which normal applications don't. In one type of attacks, the attacker tries to take the control of VMM which is running on the host machine. Typically the target of this attack is gaining access to the host machine [6].

- **Unsecure VM Migration**

One of the useful features of virtualization which is widely being used in cloud computing is live migration of VMs between two hypervisors. Even though in some virtualization technologies, VMs are encrypted for migration but most of the time the content of the VMs are not protected well enough. Some vulnerabilities have been seen on Xen and VMWare products [6].

In a project, they have managed to modify the memory of a VM during live migration [10]. They have developed a tool named Xensploit that is able to perform *a man in the middle* (MiTM) attack in live migration. To mitigate the probability of this attack, performing mutual authentication between the source and destination VMM can be done. Also using virtual network or a separate and secure physical network can be helpful [11]. An improved version of virtual Trusted Platform Modules (vTPM) protocol has been proposed for secure migration of VMs [12].

- **Resource Allocation**

As we mentioned earlier, the VMM is responsible for allocating system resources among the VMs and any resource usages must be intercepted by VMM. If an attacker takes control over the resource allocation, he can take most of the resources for one VM causing the entire virtual environment goes out of service and some type of *denial of service* attack happens [11].

C. External Security Challenges

In previous cases, malicious activities originated within the virtual environment, either guest or host machine or VMM. But a virtual environment is also vulnerable to external threats. In this section we look at vulnerabilities that can be used by remote attackers.

- **Rootkit Attacks**

Rootkits are malware that are able to be present in a computer system without being detected and be hidden to the main parts of the system. Rootkits can be used by a remote attacker in different layers of virtualization [1]. For example, Blue-pill is an x86 architecture based virtualization rootkit that targets Microsoft Windows Vista. This rootkit is able to run inside an operating system in a virtual machine and take control the computer and act as a hypervisor and be an access point for other malwares [13].

- **Malicious Code Injections**

There are different types of vulnerabilities in software that might cause a malicious code injection be possible. For code injection, buffer overflow and accepting command line inputs are common. In these attacks, attacker tries to penetrate to VM and inject a malware code in different levels of virtualization [1].

D. Management Security Challenges

Cloud computing with demand on different types of services like Software as a Service (SaaS) and Infrastructure as a Service (IaaS), makes the management of virtualization environment and virtual machines very challenging and cause some security problems such as the followings.

- **VM Mobility**

VM mobility in cloud computing lets users importing a customized VM image into the infrastructure service. Since the content of VM can be transferred, this may lead to spreading the miss configurations and make sensitive data vulnerable. As mentioned previously in unsecure VM migration, this can cause a man in the middle attack [6], [14].

- **VM Sprawl**

Because creating new VMs can be easily done in couple of minutes, after a while there will be a lot of VMs with different types without proper IT management. VM Sprawl is one of the biggest issues that data centres are facing. As the number of VMs increases, it makes the defining of rules and access permissions more complex and some rules might be overlooked. In these situations, service providers must ensure security of the services and the users keep their VMs secure and up to date [6], [15].

A management system has been proposed for managing virtual machines that allows to control the access to the versions of VMs and filtering and checking the integrity of VM file [16].

IV. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Both penetration testing and vulnerability assessment are for testing the security and identify the weak parts of a system, but there is a difference between these two. During vulnerability assessment usually, the computer systems are scanned by some tools to detect the vulnerable areas of that systems while penetration testing goes deeper and during its process they actually perform a real attack to see how the system work under a real attack and a report is created that specifies whether the attack was successful or not and it may contain details about the attack.

There are different types of penetration testing and we can categorize them based on their scope (attack by an insider or an external source) or what an organization wants to test. Generally, there are two approaches in penetration testing, Black-box and White-box. The difference of these two is the amount of information that the tester knows about the system [2].

A. Black-box testing

In this type of penetration testing which is also called “external testing” or “remote testing”, the tester has no prior knowledge about the infrastructure by deploying the number of real-world attack techniques. For example the tester will be provided with only the website or network IP address of organization [2].

B. White-box testing

In White-box testing, the tester has prior knowledge of some components of system like details of operating system, network IP address scheme, application code, and sometimes even the passwords. The main goal of this testing is to verify the integrity of organization network and reduce the risk from internal attacks [2].

C. Virtualization Security Assessment Tools

There are many tools and software for security assessment and penetration testing which we can use for virtualization and other environments. We can consider a hypervisor like an operating system with some services and open ports running on a network, in this case there lots of tools which can be used to assess the hypervisor. Some tools are needed to run from a guest VM in a hypervisor.

- **V.A.S.T.O and Metasploit**

Metasploit is not just a vulnerability assessment tool but also a penetration testing framework for exploring vulnerabilities and exploiting them. Metasploit contains lots of modules for security assessments and attack simulations. Performing real attacks typically includes discovering vulnerabilities by some scan tools and finding appropriate attack tools for them which can be complex for many testers whose do not have enough experience in this field. The goal of Metasploit is to facilitate this process [17].

V.A.S.T.O is a penetration testing tool specific to virtualization, it has a set of modules that can be added to Metasploit framework. V.A.S.T.Os modules are mostly for VMWare and Xen products. Each module is for performing an assessment scan or an attack. The followings are some of the important modules of V.A.S.T.O [18]:

1. Abiquo_guest_stealer: Performing path traversal attack to escape to the host machine in Abiquo.
2. Abiquo_poison: Sniffing and performing MiTM attack in Abiquo communications.
3. Vmware_guest_stealer: Path traversal attack in VMWare.
4. Vmware_login: Performing brute-force attack to login to a VMWare server.
5. Vmware_lurker: Code execution during a MiTM attack in VMWare.
6. Vmware_version: For fingerprinting and extracting the details of any VMWare server.

For some attacks, multiple modules from V.A.S.T.O or Metasploit's own modules may be needed.

- **VM-Informer**

Unlike V.A.S.T.O which lets the tester to select the penetration test type, VM-Informer assess the security of virtual environment based on security policies and is not developed as an intruder's point of view. Policies are basically security benchmarks which can be modelled according to the requirements. After scanning the environment, it provides a report that identifies the security and insecurity of the environment. VM-Informer audits the following vulnerabilities [18]:

1. Miss configuration
2. Lack of security patches
3. Improper network scheme
4. Weakness in management layers

- **Nessus**

Nessus is one of the vulnerability assessment tools which is able to scan multiple host at the same time and evaluate the scan result with known dynamic vulnerability databases. According to Nessus developer, its aim is to be a "free, powerful, up- to-date and easy to use remote security scanner". The main part of Nessus is its plugins, written in either C language or NASAL (a script language specific to Nessus). Nessus can automatically scan the hosts and thus it is a useful tool when there are lot of servers and hosts. Some of the Nessus plugins not only detect the system vulnerabilities, they also provide some instruction for remediation. Nessus also let its users to add their own plugin which are written in NASAL.

Nessus can be used to discover vulnerabilities like DoS, code execution, buffer overflow, VM escape [19], [20]. For vulnerability assessment of VMWare with Nessus there is a capability that let you login with SOAP API which gives the tester more information about the virtualization environment and its vulnerabilities [19], [20].

- **Ettercap**

Ettercap is a multipurpose network sniffer/interceptor/Logger for LAN networks. When it lands on a network switch, it is able to see all the communications are being passed by the switch and exploits them. Ettercap can be used for multiple types of man middle attack. It has some features that can be used during the attack [21]:

1. Character injection
2. Packet filtering
3. Automatic password collection for many common network protocols
4. SSH1 support
5. HTTPS support
6. PPTP suite
7. Kill any connection

In virtualization assessment this tool can be used to sniff and manipulate the messages sent between management client and hypervisor management API [20]**.**

- **Hydra**

Hydra is a tool for password cracking using brute-force attack. A brute-force attack consists of an attacker trying many passwords with the hope of eventually guessing it correctly. Hydra supports many online services like POP3, HTTP, IMap and etc. In Virtualization Hydra can be used to test the brute force attack on the password authentication by examining whether there is any prevention mechanism in place [22], [20].

- **NMap**

NMap is a tool for scanning a range of IP addresses, identify active systems, discovering the open ports and what operating systems are running on those systems. Like other scanning tools NMap can be used by network administrators to find the vulnerabilities in the network or by an attacker for malicious activities. Typically, in security assessment of an environment first of all we need to gather information about the system we are trying to examine. We need to know what services are running on the system or the hypervisor and in what version in order to find proper vulnerabilities and methods to exploit them. NMap is of the best tools that can be used for information gathering of penetration testing [23].

- **TCP-Replay**

In the *man in the middle* attacks, captured packets can be used for a replay attack. A replay attack consists of sniffing a communication between two parties and after capturing sensitive packets like password or password hashes it uses this packet to authenticate to the system later. In virtualization environment if a deletion of VMs are allowed, this environment probably is vulnerable to replay attack [20], [24].

- **Cain&Able**

Cain&Able is a tool for performing ARP-Spoofing which is also a MiTM attack. The aim of this attack is monitoring the packets that are sent to a machine or sent out by the machine. This tool can redirect the communication between two machines to be passed from the attacker’s machine first and then goes to its destination. In virtualization this tool can be used to assess the security of communication between management client and hypervisor management API [20].

From these tools, some of them like V.A.S.T.O or VM-Informer are specific to virtualization, but most of them are general tools which do have applications for virtualization environments as well. Another difference is that for example V.A.S.T.O and Metaslpoit are penetration testing tools which are able to perform actual attacks and some manual steps are need using them while Nessus is a scan tool that detects vulnerabilities of a system. Regardless of what is the type of the tool and how can it assess a particular vulnerability we just consider a tool is able to assess a vulnerability, whether it can just detect the vulnerability or it is able to exploit them too. Table 1 shows what tools related to what vulnerabilities.

Table 1: Virtualization Security Assessment Tools and Vulnerabilities

	V.A.S.T.O	NESSUS	CAIN&ABLE	TCP-REPLAY	HYDRA	ETTERCAP
VM Escape	*	*				
VM Hopping		*				
MiTM	*	*	*	*		*
Denial of Service	*	*				
Code Execution	*	*				
Unauthorized login	*	*		*	*	
Rootkits	*					

Table 2: V.A.S.T.O for Penetration Testing of Virtualization

	VMWARE	XEN	ABIQUO	ORACLE-VM
VM Escape	*		*	
VM Hopping				
MiTM	*		*	
Denial of Service	*			
Code Execution	*	*		*
Unauthorized login	*	*		
Rootkits	*			

Table 3: Nessus for assessment of virtualization products

	VMWARE	XEN	K.V.M
VM Escape	*	*	*
VM Hopping	*		
MiTM	*	*	
Denial of Service	*	*	*
Code Execution	*		*
Unauthorized login	*		
Rootkits			

Table 2 and 3 show the relation of V.A.S.T.O and Nessus for assessment of vulnerabilities based on virtualization products. The rest of the tools are kind of used for assessment of networks or can be used in combination to perform penetration testing.

V. DISCUSSION

To make the systems and environments secure for small companies that do not want to spend too much for security, the security assessment could be only exploring vulnerabilities, take a report and try to fix the issues based on their priorities. Tools like Nessus would be helpful for such purposes, because it is easy to use, and you can check your systems periodically, and it also provides useful information for remediation of the issues. VM-Informer is also can be used in these situations. But in companies that security has a big role they may want to go even deeper and find out too much about their systems, how their systems can be a target of attacks, how they react to that attacks and how much faster they can recover after. For this job, someone that has enough experience to perform the penetration testing is needed and the process needs knowledge about the system and tools.

Some of the tests are tricky and most of the time the tester need to use a bunch of tools in combination. For penetration testing a tool like NMap can be used to scan the services and ports, the operating systems version and other information at information gathering phase. Beside Metasploit sniffing modules Ettercap or Wireshark are useful tools for sniffing and checking the hypervisor's network connections. Metasploit has also some modules that can be used for password cracking as well as Hydra itself.

In conclusion, as shown in Table 4, for a simple assessment Nessus or VM-Informer can be run to check the virtualization environment to find out what vulnerabilities are present, this scan can be used as a first step of a penetration testing operation too. We can use the information of the vulnerabilities to search and find appropriate tools to perform penetration testing.

Table 4: Tools for Vulnerability Assessment and Penetration Testing of Virtualization

	RECOMENDED TOOLS
Vulnerability Assessment	Nessus, VM-Informer
Penetration Testing	Nessus, VM-Informer, Metasploit, Ettercap, Hydra, Cain&Able, …

VI. CONCLUSION

Although the virtualization is very practical in data centres and cloud computing, but it is necessary to assess its impacts on security components. In this paper we have tried to evaluate virtualization technology with security perspectives. Table 5 presents our reviewed virtualization security benefits and vulnerabilities and some recommended tools which can be used in security assessment of virtualization.

Table 5: Summary of virtualization security benefits, challenges and tools

Virtualization Security Benefits	• Better and faster recovery after attack • Patching safer and more effective • Cost effective security devices e.g. virtual IDS • External monitoring by VMM • VM is a safe place for testing malwares	
Virtualization Security Challenges	Guest VM Challenges	• VM Hopping • VM Escape • Side Channel Attacks • VM Alteration • VM System Restore
	Host VM and VMM Challenges	• Hypervisor Hyper-jacking • Unsecure VM Migration • Resource Allocation
	External Challenges	• Rootkit Attacks • Malicious Code Injections
	Management Challenges	• VM Mobility • VM Sprawl
Virtualization Security Assessment tools	• V.A.S.T.O and Metasploit • VM-Informer • Nessus • Ettercap • Hydra • NMap • TCP-Replay • Cain&Able	

VII. REFERENCES

[1] K. Pooja, R. Nagpal, and T. P. Singh, A Survey on Virtualization Service Providers , Security Issues , Tools and Future Trends, *Int. J. Comput. Appl.*, vol. 69, no. 24, pp. 36–42, 2013.

[2] N. Shrestha, Security Assessment via Penetration Testing: A Network and System Administrator's Approach, Master's thesis, Univ. OSLO, 2012.

[3] E. R. Rasmussen, Reducing IT Costs and Increasing IT Efficiency by Integrating Platform-Virtualization in the Enterprise, Univ. Oregon., vol. 1277, no. February, 2009.

[4] R. Randell, Virtualization Security and Best Practices, RSA Secur. Conf., 2006.

[5] G. Obasuyi and A. Sari, Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment, *J. Commun. Netw. Syst.*, no. July, pp. 260–273, 2015.

[6] A. Mahjani, Security Issues of Virtualization in Cloud Computing Environments, Master's thesis, Luleå Univ. Technol., 2015.

[7] S. Zahedi, Virtualization Security Threat Forensic and Environment Safeguarding, Linnéus Univ., Degree project, 2014.

[8] A. Yu and D. Brée, Side channel Attack-Survey Joy, *Inf. Technol. Coding*, vol. 1, no. 4, pp. 54–57, 2004.

[9] J. Kirch, Virtual Machine Security Guidelines Version 1.0, *The Centre for Internet Security (CIS)*, 2007.

[10] J. Oberheide, E. Cooke, and F. Jahanian, Empirical exploitation of live virtual machine migration, *Proc. BlackHat DC* , no. VMM, 2008.

[11] A. Tayab et al., Virtualization and Information Security A Virtualized DMZ Design Consideration Using VMware ESXi 4.1, Unitec Institute of Tech, New Zealand, vol. 2, p. 89, 2012.

[12] X. Wan, X. Zhang, L. Chen, and J. Zhu, An improved vTPM migration protocol based trusted channel, *Int. Conf. Syst. Informatics, ICSAI 2012*, no. Icsai, pp. 870–875, 2012.

[13] U. Gurav and R. Shaikh, Virtualization – A key feature of cloud computing, *Int. Conf. Work. Emerg. Trends Technol.*, no. Icwet, pp. 227–229, 2010

[14] K. Benzidane, S. Khoudali, and A. Sekkaki, Secured architecture for inter-VM traffic in a Cloud environment, *2nd IEEE Lat. Am. Conf. Cloud Comput. Commun. LatinCloud 2013*, pp. 23–28, 2013.

[15] H. Tsai, N. Chiao, R. Steinmetz, and T. U. Darmstadt, Threat as a Virtualization's Impact on Cloud Security, *28th IEEE Int. Conf. Data Eng.*, no. February, pp. 32–38, 2012.

[16] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, Managing security of virtual machine images in a cloud environment, Proc. *2009 ACM Work. Cloud Comput. Secur. - CCSW '09*, no. Vm, p. 91, 2009.

[17] B. Greenwood, An Introduction to Metasploit Project for the Penetration Tester, SANS Institute report, https://cyber-defense.sans.org/resources/papers/gsec/introduction-metasploit-project-penetration-tester-107151 [Accessed: June 2018].

[18] S. Chauhan, Hacking VMware with VASTO, Infosec Inst. report, http://resources.infosecinstitute.com/virtualization-security/#gref. [June 2018].

[19] J. Mitchell, Proactive Vulnerability Assessments with Nessus, SANS Inst. report, https://www.sans.org/reading-room/whitepapers/auditing/paper/78. [Accessed: June 2018].

[20] A. Thongthua and S. Ngamsuriyaroj, Assessment of hypervisor vulnerabilities, Proc. - *Int. Conf. Cloud Comput. Res. Innov. 2016*, pp. 71–77, 2016.

[21] D. Norton, An Ettercap Primer, SANS Inst. report, https://www.sans.org/reading room/whitepapers/tools/paper/1406 [Accessed: june 2018].

[22] C. Yiannis, Modern Password Cracking : A hands-on approach to creating an optimised and versatile attack, Inf. Secur. Group, R. Holloway, Univ. London, no. May, 2013.

[23] T. Corcoran, *An Introduction to NMAP*, SANS Inst. report, https://www.sans.org/readingroom/whitepapers/tools/paper/72 [Accessed: June 2018].

[24] A. Hussain, Y. Pradkin, and J. Heidemann, Replay of malicious traffic in network testbeds, *IEEE Int. Conf. Technol. Homel. Secur. HST 2013*, pp. 322–327, 2013.