Virtual Machine Escape in Cloud Computing Services

Hesham Abusaimeh
Associate Professor in Computer Science
Middle East University, Amman, 11831 Jordan

***Abstract*—It's of axioms; every progress that is devised in the field of facilitating daily life through technology is matched by many complications in terms of the methods that led to the creation of these inventions and how to maintain their sustainability, consistency, and development. In digital world that became not only as axiom of its nature, but it is now one of the main inherent features that define digital technology. Whereas Major international companies are in a big race to produce the new development and invention of their products to be supplied to markets, and all of that should be conquered within not more than a year. The immersion in that big race has to be armed with patience and deep breath.**

***Keywords*—Cloud computing; virtual machine escape; cloud security; impact of VM escape; VM escape counter measures; VM escape nature**

I. Introduction

With virtualization world, that accelerating, competitive, and pervasive environment, you would be plagued and dominated by many restrictions and vectors in terms of acquisition of business solutions. Hence, it's effortless to build a compute of the given resources in virtualization atmosphere, in other word; we can build virtual storages, virtual CPU's, virtual memory, etc. as much as we need, where & when needed within minutes or seconds [1].

This steady, fast, exaggerated and easy increase in the nature of virtualization which is intrinsic characteristic of it compels us to dealing with a proxy-managed property.

However, in virtualization each step has been made could expose us to be in the middle of a mud. Yet, we could characterize virtualization as a muddy, very flabby, slimy texture of logical components (Virtual Machine, Hypervisor, O.S.), leading to be parachuted uncovered in a confrontation with that exaggerated sprawl/stretching Orbit [2].

With all of the above, it's uneasy to hold that emulated components of virtualization entity close enough together to be functioned, give rise to a notorious vulnerability in Virtual Machines.

As a result, emerging of a real threat of breaking out the Virtual Machine and establish a direct interaction with the hypervisor, or with the host operating system, or create communication with the hardware itself, is called Virtual Machine Escape [3].

II. Research Methodology

Although most of the threats and flaws identified in physical hardware of Data Center are the same in Virtual Data Centre and any researcher could effortlessly find many topics cover these threats and concerns of cloud computing. However, when we have decided to prepare this paper, we have identified a very important question related to the rarity of scientific topics covering VM Escape; which encouraged us to proceed with probing this type of threats and trying to neutralize its patterns and shapes it could has.

In this paper we have strived to trace every piece of information and evidence about VM Escape. This collected information has been cited from well-mannered scientific researches published in prominent data basis. Hereinafter, we shall go through scanning and analyzing various issues regarding Virtual Machine Escape, to provide an overview of the VM Escape threat. Yet, this paper could not represent the ideal solution to prevent or mitigate the threat. Nonetheless, it provides a general understanding of the VM Escape threat and how it could be avoided to maintain Business Continuity of cloud computing.

To recognize the threat clearly, one should have his bird's eye view of the Virtual Architecture on various level as shown in Fig. 1.

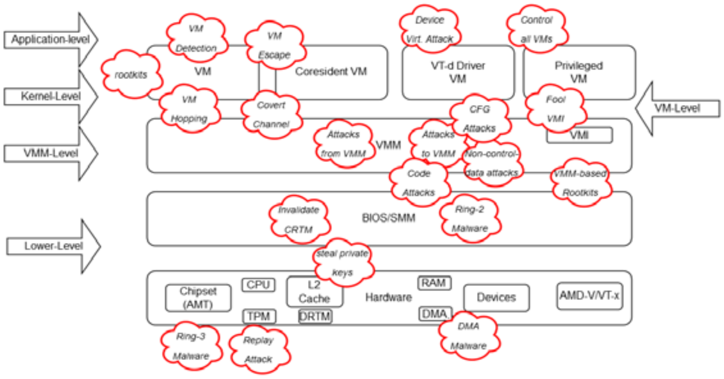

Fig. 1. Summary of some Attacks at the Various Levels [2].

III. Terminology

- Host: is a platform in virtualization environment running hypervisor software. All systems in virtualization run atop the platform of host hypervisor.
- VM, Virtual Machine, Virtual guest, usually called a Virtual Machine, is any system running the extracted environment which shall represent virtual model. Essentially, Virtual Machine is a group of files that exemplifies a hardware-based computing platform, is addition to configuration components, memory and storage altogether.
- Shared Folder: shared folders of malware that give permission to users to send/receive data between the non-virtualized system (Host) and a virtualized system (Guest).

IV. Virtual Architecture

- Traditionally, one operating system (OS) is deployed to each system (physical Hardware).
- Hypervisor is software authorizes multiple operating systems (OSs) to be run on hardware.
- As shown in Fig. 2, there are two types of Hypervisor:

1) Type 1 (Bare-metal hypervisor).
2) Type 2 (Hosted hypervisor).

- Virtual Machine: Virtual machine (VM) is a simulation of a computer system.
- There are three techniques of virtualizations as shown in Fig. 3; Full, Para, and Hardware Assisted Virtualization.

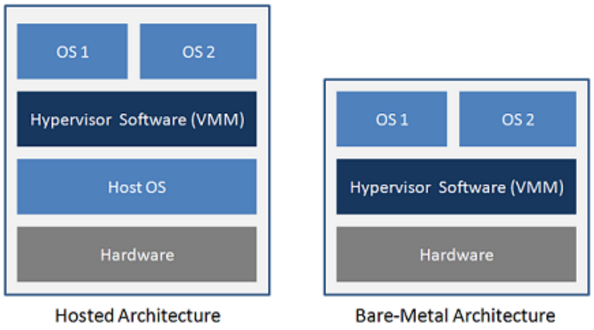

Fig. 2. Demonstration of Hypervisor Types [3].

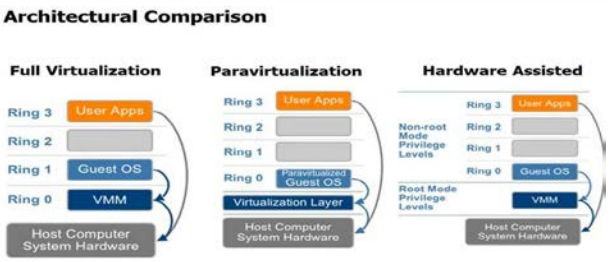

Fig. 3. Demonstration of the Virtualization Types [3].

V. History of VM Escape

A. Sand Table

Militarily, sand table is a method in which some of the military commanders who shall involve in attack or defense against the enemy use sands for modeling the friend and enemy forces; each commander has to demonstrate his predictions from the enemy's point of view, and how could the enemy uses the fragile points for potential attack.

B. Origin of VM Escape

In 2007, at Sansfire conference held in Washington DC, Tom Liston and Ed Skoudis (Senior Security Consultants) have demonstrated a concept of VM Escape. They have modeled several tools Highlighted that VM Escape might be occurred like VMchat, VMcat, VM Drag-n-Sploit and VMftp [4].

VI. VM Escape Nature

While the Hypervisor stands as barrier separating between the hardware resources and the Virtual Machines, offering a full isolation for the Virtual Machine, VM Escape is a compromise of the virtualization environment by an attacker who could exploit the virtual machine runs above the hypervisor. As a result, the VM Escapes from the isolation sphere. The possibility of such an attack is the attacker could run a code on a virtual machine, allowing an operating system running inside the hypervisor to be broken out and interact with it directly. This kind of attack might allow the attacker to have an access to the host operating system in addition to each virtual machines working on that host.

At Sansfire Conference experts were weighting that most of Virtual Machine Escape vulnerabilities are sourced to a type of Directory Traversal Attack [4].

There are number of Virtual machine escape types that may occur depending on the tools used to trigger Virtual Machine Escape attack [5], these tools are:

VMchat: It is plain chat software utilizes the VMware hypervisor communication channel as a backdoor to send messages between guest's operating systems exclusively or between guest's operating system and the host. A special code to be installed is unnecessary.

Otherwise speaking, an injection of a Dynamic Link Library/DLL attack could take advantage of VMware running on the host operating system, granting a license for the App. running on the host to access the memory of the guest's VMware machine, when this took place, the memory buffer will be used as a shared buffer, a shared buffer that provides a mutual environment to initiate communication between the host machine and client. This tool will not have the Virtual Machine to be escaped completely; but enables penetration the boundary between host machine and VMware.

VMcat: This could be defined as a VMchat extension tool to send simple (stdin) and (stdout) files between the mutual environments created in VMchat which could be managed to pipeline a command shell between hosts and guest.

VM Drag-n-Sploit: In this case, a VMware component on the guest called (VMwareService.exe) could be mutated in its form of nature; experts could perceive and shift all data passing through the mutual environment. This leads to manipulate the data being towed from gust to host using function built in VMware station called “drag-n-drop”. The experts used “drag n drop” to prompt command shell from the host to guest.

VMftp: As long as shared folders are enabled, a flaw discovered in iDefense Shared Folder could enables the VMftp tool to take advantage of a user on any guest, regardless of its privilege could read and write to the host.

VII. Escape Classes

There are three main escape classes could be traced in Virtual Machines, these classes are specified depending on the direction pursued by VM’s, as follows:

VM escape to host: breaching the isolation between host and virtualized environment. This happens when code from a VM runs inherently on the host machine apart from any control of the VMM. Since there are weaknesses or flaws in the VMM, attackers aim to attacking virtualized devices, caches of CPUs and Direct Memory Access/DMA to acquire an access to the memory of the host straightly [6].

VM escape to VM: as shown in Fig. 4, a rule of each VM should not change or examine the data of other VM’s is essential. When this rule is breached, it’s called VM escape to VM [6].

VM virtual network escape: as shown in Fig. 5 the breach occurs at the virtual network zone rather than general I/O, namely a VM dodging intended network boundary [6].

As shown in Fig. 6 and unlike other cloud attacks which most have one, two or three impacts on cloud, VM Escape attack could have impacts on confidentiality, integrity, authentication, authorization or even availability of Cloud [7] [8] ; and as long as the hypervisor represents a single point of failure component [9]; and there are types of VM Escapes in which attacker could take control over the whole hypervisor [10], consequently; VM-escape attack is considered to be one of the most catastrophic threats to the Cloud [11]. The seriousness of the attack not only lies in sophistication, it is an ad-hoc and hard to get detected as well [10].

As for aforementioned reasons, Virtual Machine Escape threat has to be solved urgently. It’s good to mention that VM Escape can affect the IaaS layer [12].

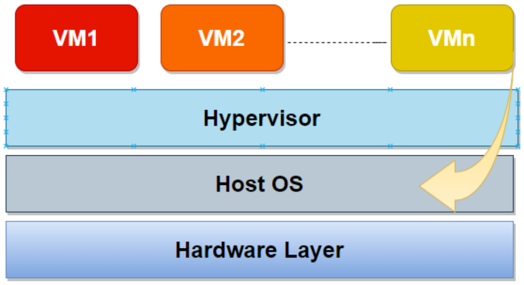

Fig. 4. Demonstration of VM Escape to Host.

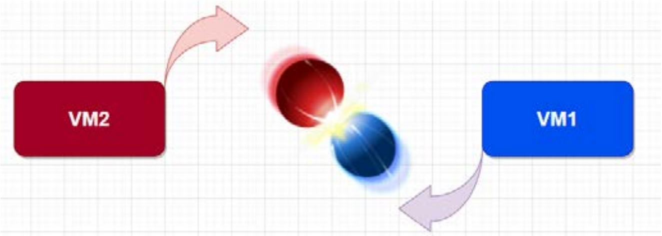

Fig. 5. Demonstration of VM Escape to VM.

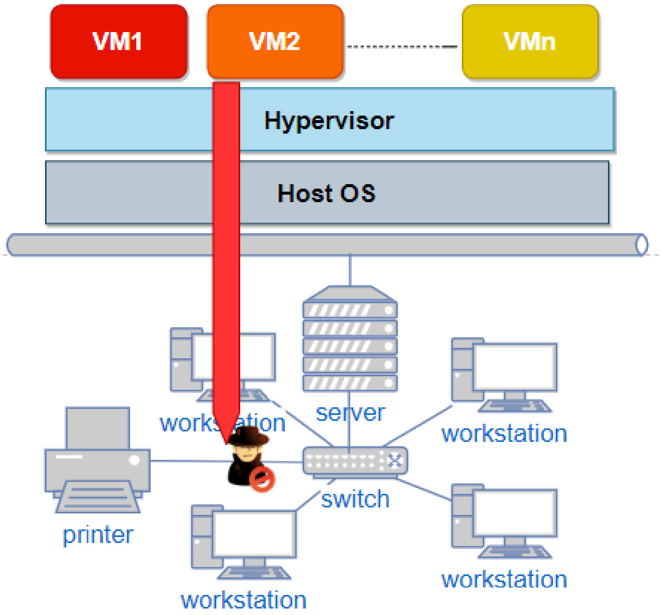

Fig. 6. Demonstration of VM Escape to Network.

Generally, it is of importance; theoretically and practically surveying modality to provide a safe environment to secure this significant sector titled cloud computing and to deter malicious attacks.

VIII. Counter Measures

To some extent, VM Escape attack stands still as an unresolved lofty threat that VM may encounter [7]. Moreover, mitigating or preventing the attack (based on its nature) may require fortification of other cloud components including physical resources rather than VM itself [10].

Nonetheless, there are many approaches security specialists have to keep track to maintain minimum extent to secure VM’s.

In general, a penetration test to be performed to have a general assessment of virtualization environment security. This considered as an essential approach to conduct [9].

Furthermore, the adoption of techniques and methods to - hypervisor-hardening is inevitable [10].

Thwarting Virtual Machine Detection is another approach to secure VM’s from malicious attacks lead to VM Escape; especially there are a growing number of malicious programs conveying code to recognize the presence of virtual environments [13].

Also, hindering of VM Escape attack requires software engineering, Patching and formal verification [7].

Moreover, checking the security & integrity of the Hypervisor; harden and secure the Guest OS; isolate & secure the virtualized network; achieve a real-time Zero-day malicious activities detection; put other controls and security policies in place and restore guest VMs to a clean state automatically [8].

The cloud providers have to provide secure, reliable cloud computing environment. They are bundled to endeavor all possible executions to achieve that goal.

Therefore, Trusted Virtual Domain (TVD) is another approach to secure cloud from VM Escape incidents [6].

Other approaches could be pursued are based on Memory Introspection. A process through which a hardware-based approaches to obtain the physical memory of the host machine in real time, thereby; diagnoses of the security of the host machine and VM could be examined. Furthermore, a new approach to analyze the forensics of VM memory rested on the virtual machine control structure (VMCS) has been triggered. Through scrutinize the host machine memory, the operating VMs could be recognized and the high-level of their semantic data could be rebuilt. Eventually, active malignant in the VMs could be detected in an appropriate time. Moreover, through interpreting the memory quintessence of the VMs and host machine, VM escape could be detected by observing the abnormal attitude pattern of the host machine. So far, a relevant written work to solve the problem of VM escape detection has not been found yet [14].

On the other hand, some experts put forward a restriction access to the Virtual Machine’s resources by defining new policies to manage Access Control/Access Control Model. A new system to harden Open Stack called SOS was proposed. SOS comprised of a framework which apply wide layers of security measurements and define trust limits on compute nodes. They have generated a Mandatory Access Control (MAC) to limit the communications between different components. These policies shall be originated automatically.

Nevertheless, this method is not convenient for instant deployment, because running cloud platforms should be modified [11].

The experts proposed several actions to be taken to handle VM Escape using MAC, each method has its advantages and disadvantages, below we shall provide a brief of the tools invented to solve VM Escape based on Mandatory Access Control.

An application of a MAC framework shall be applied to multi-level security (MLS) in Xen based on a Virt-BLP model (Bell-La Padula) [11]. Nevertheless this model secures the communication between VMs; it does not address the problem of interaction between VMs and the Hypervisor.

A design of multilevel security access control V-MLR related to the mandatory access control. This tool provides secure communication environment for VMM and VMs. Also; it provides an update of the acquired information in VMM concurrently when changes on that information occur in VMs. Yet, this tool is related to Xen system of Virtual Machines.

Construction of multilevel security on the basis of BLP model. The level of security in this tool could be changed dynamically, especially when users read critical data. This tool guarantees the aspect of users become unable to leak these critical data they have read. However, results of effectiveness of this model still foggy. The BLP model is originated for the conventional system rather than virtualization system. In spite of both virt-BLP & Prevent Virtual Machine Escape (PVME) [11] are based on the BLP model, they tend to share different approaches though. As example, the PVME model used in full virtualization and principally handles the security problems between Hypervisor and the VMs with regard to the subject of communication. Otherwise, virt-BLP is implemented in Xen VM’s, whereas Xen represented as Para virtualization; it primarily addresses the VM’s communications security [11].

Also, On the other hand, to solve Escape problems, the interaction of host/guest should be configured properly [15].

However, prevention of the VM escape to host & VM escape to VM classes requires a combination of VMM patching, host security procedures, and methods to disclose the malicious code in the VM.

As long as these two classes enable the attacker to acquire the access to data; It is of logic to be aware that the risks could be mitigated when the specialists seek for encryption of the high value of storage altogether with the assets of communication in order to avoid the disclosure of valued data in case they have been compromised. Specifically, storing encrypted database records on virtual disk shall be secured in case of compromising or reading the file [6].

Furthermore, the Adoption of symmetric/asymmetric algorithms to have encryption of data is a common method to protect the data in Virtualized infrastructure; the most common encryption approach is Service Level Agreements (SLAs) [16].

Other common approaches to secure Virtualized infrastructure could be outlined by firewall service, a virtual firewall (VF) operating within virtual environment could provide constant filtering of packet and monitor the services provided by physical firewall. To achieve this goal, VFs residing at the hypervisor should be applied on the VMM; as long as the VMM is responsible for apprehending malicious Virtual Machine activities including packet insertion. A modification to be applied at the kernel of the physical host hypervisor to enable the installation of modules or hooks granting the VF system an access to the information of VM and an unreserved access to the virtual network in addition to moving packets between VMs at virtualized network interfaces. Yet, these hooks or modules could be used to execute all functions of firewall like dropping, packet inspection, and forwarding. Yet, all of these functions to be performed without palpating the virtual network [16].

As long as the VM Escape attack -In many cases- are based on breaching the isolation between host and virtualized environment or between VMs, therefore keep an eye on the measures preventing this from happening in the isolation property is not a waste of time. Many approaches are available to address this issue [17].

Since the hypervisor represents a probable surface to trigger an attack between two virtual machines, so the removal of VMM to be considered as a radical solution to get rid of this surface through abandoning the hypervisor.

This could be implemented through the adoption of hardware assisted virtualization and placing number of restrictions on virtualization conditions.

However, when VMM removal is implemented, virtualization infrastructure shall lose certain features, as example; VM's became incapable to share resources (buffers, devices, memory) between them as shown in Fig. 7 [17].

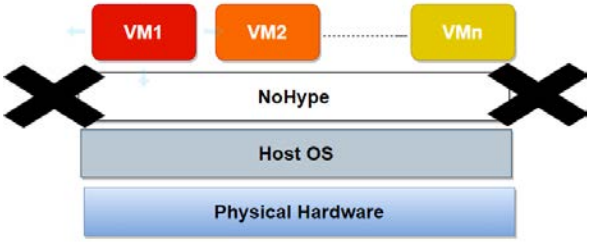

Fig. 7. NoHype Architecture [17].

IX. Conclusion

In general, this paper introduced most of the main VM Escape attacks details. Beginning from the VM Escape definition; ending with the methods undertaken to put down or soften it. Furthermore we have stopped at several tools and techniques could trigger VM Escape attack. For all that regulations listed/available to confront VM Escape attack alone or along with other possible attacks, VM Escape is such a stubborn threat cloud might come across.

As aforementioned above, there are many regulations to seek countering VM Escape attacks; and experts are in a big race to curb that vicious attack. Nonetheless; the attackers are matching their steps to level up their tools and techniques to come up with new VM Escape patterns & styles to beat these assumed preventing regulations.

Throughout the demonstration of VM Escape attack which is - as with the rest of the other VM attacks - based on a real vulnerability in VM's; in addition to the serious impact could be occurred by this type of attacks which - in some cases - threatening availability of the Cloud; taking into account other bunch of attacks that target VM's; therefore, VM shall be considered as of the most fragile component of cloud.

Definitely, experts seek to have a free of defects cloud. Ultimately, unstoppable attack requires - even though considering cauterizing the cloud-which represents the eventual medicine. Accordingly, the consideration of shifting cloud from VM's to Containers is believed to be as an enhancement for the whole cloud performance.

Recently, migration from using VM's towards an alternative option characterized by Containers is increasing [18].

Yet, while the cloud is pulsing somewhere, the danger shall be lurking and the battlefield shall persist.

Acknowledgment

The author is grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

References

[1] H. Abusaimeh, "Security Attacks in Cloud Computing and Corresponding Defending Mechanisims," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 3, 2020.

[2] H. A. H. a. S. H. Abusaimeh, "Security on cache-based side-channel attacks in cloud computing," International Journal of Emerging Trends in Engineering Research, vol. 8, no. 4, pp. 1019-1026, 2020.

[3] H. Abusaimeh, "Distributed Denial of Service attacks in Cloud Computing," vol. 11, no. 6, pp. 163-168, 2020.

[4] D. Shackleford, in Virtualization Security: Protecting Virtualized Environments, Sybex; 1 edition , (November 28, 2012).

[5] A. A. A. Ali, "researchgate.com," April 2013. [Online]. Available: https://www.researchgate.net/publication/255791810. [Accessed Jan 2020].

[6] R. H. S. Z. Michael Pearce, "Virtualization: Issues, Security Threats, and Solutions," ACM Computing Surveys, February 2013.

[7] B. T. W. M. E. W. P. X. B. K. M. P. H. d. M. &. H. P. R. Noëlle Rakotondravony, "Classifying malware attacks in IaaS cloud environments," Journal of Cloud Computing volume 6, Article number: 26 , 2017.

[8] C. Y. Y. M. J. Z. Fatma Bazargan, "State-of-the-Art of Virtualization, its Security Threats and Deployment Models," nternational Journal for Information Security Research (IJISR), vol. Volume 2, September/December 2012.

[9] N. C. A. A. Darshan Tank, "Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison," International Journal of Information Technology , 2019.

[10] S. Zhang, "Deep-diving into an easily-overlooked threat: Inter-VM attacks," Kansas State University.

[11] Z. L. S. C. a. W. S. Jiang Wu, "An Access Control Model for Preventing Virtual Machine Escape Attack," MDPI, 2017.

[12] K. R. Dinakar, "A Survey on Virtualization and Attacks on Virtual Machine Monitor (VMM)," International Research Journal of Engineering and Technology (IRJET) , vol. 06, no. 03 , Mar 2019.

[13] E. S. Tom Liston, "On the Cutting Edge: Thwarting Virtual Machine Detection," ©2006. [Online]. Available: https://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf. [Accessed Jan 2020].

[14] X. M. L. W. L. X. a. X. H. Shuhui Zhang, "Secure Virtualization Environment Based on Advanced Memory Introspection," Security and Communication Networks, vol. 2018 , p. 16 pages, 20 March 2018.

[15] J. S. Reuben, "A Survey on Virtual Machine Security," in Security of the End Hosts on the Internet, Seminar on Network Security , 2007.

[16] A. F. S. Althobaiti, "Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment," Journal of Information Security, January 2017.

[17] E. A. Y. D. M. K. V. N. Ivan Studnia, "Survey of Security Problems in Cloud Computing," Nov 2012. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00761206/document. [Accessed Jan 2020].

[18] A. F. R. R. J. R. Wes Felter, "An Updated Performance Comparison of Virtual Machines and Linux Containers," IBM Research Report, Austin, TX, 2014.

[19] D. S. &. E. Lupu, "Evolution of Attacks, Threat Models and Solutions for Virtualized Systems," ACM Computing Surveys, vol. 48, February 2012.