National College of Ireland

Enhancing Virtualization Security in Oracle VirtualBox: Investigating VM Escape Vulnerabilities and Mitigations

MSc Research Project
MSc Cybersecurity

Joshua Chakko Jacob
Student ID: 21124701

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Joshua Chakko Jacob
Student ID:	21124701
Programme:	MSc Cybersecurity **Year:** 2023
Module:	Research Project
Supervisor:	……
Submission Due Date:	16-09-2023 ……
Project Title:	Enhancing Virtualization Security in Oracle VirtualBox: Investigating VM Escape Vulnerabilities and Mitigations
Word Count:	7232 **Page Count** 18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Joshua Jacob ……

Date: 14-08-2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Virtualization Security in Oracle VirtualBox: Investigating VM Escape Vulnerabilities and Mitigations

Joshua Chakko Jacob
21124701

Abstract

Virtualization has transformed computing landscapes, enabling multiple operating systems to run on a single physical host, often using hypervisors like Oracle VirtualBox. However, this advancement introduces security challenges due to shared resources, such as RAM and storage (Administrator., 2013). This research project focuses on virtualization security within Oracle VirtualBox, particularly vulnerabilities leading to Virtual Machine (VM) escape. It delves into risks linked to misconfigured shared folders between the host and guest OS. The study begins by explaining virtualization security concepts and the impact of shared folder misconfigurations (*Misconfigured Cloud Services Pose High Security Risks for Organizations - Wiadomości bezpieczeństwa*, no date). It demonstrates a scenario where a Guest OS interacts with the Host OS via a shared folder, inadvertently exposing vulnerabilities that enable unauthorized code execution on the host by the Guest OS. To mitigate these threats, a security certificate requiring authorization for host system actions initiated from the Guest OS is proposed. Experimental evidence highlights the effectiveness of this approach in enhancing security. This research addresses vulnerabilities in Oracle VirtualBox, contributing to the understanding of virtualization security. It emphasizes the significance of securing shared folder communications, offering insights into VM escape risks, and presenting a practical solution to prevent unauthorized actions. The project bridges theoretical vulnerabilities with real-world solutions, underscoring the critical importance of virtualization security. This work serves as a valuable resource for IT administrators, researchers, and practitioners aiming to establish secure virtualized environments:

1 Introduction

Virtualization, a pivotal technology in modern computing, has revolutionized the way systems are designed, deployed, and managed in enterprises as well as development environments. It enables the efficientutilization of physical resources by abstracting them into virtual entities, allowing multiple operating systems (OS) to coexist on a single physical host. Efficient utilization of the resources is one of the core foundations for the need for virtualization such that the requirement to allocate multiple systems on a single host system is always more cost-effective as compared to investing in host system for every individual application, therefore from a financial standpoint, virtualization ensures that frugal utilization of the resources is ensured from the host system. Though the concept of virtualization is almost 53 years, it was believed to have its origins in the late 1960s to early 1970s from IBM mainframes (*1.1.1. Brief History of Virtualization*, no date) which found widespread adoption in development environments, cloud computing, and server consolidation, offering flexibility, scalability, and cost savings (*5 Benefits of Virtualization*, 2021).

One of the most prominent hypervisors facilitating virtualization is Oracle VirtualBox, which is a form of type 2 hypervisor which means that the virtualization layer is a software that runs on the host operating system (*Hyper-V vs VirtualBox: In-Depth Comparison*, 2018), there are other products in the market such as VMWare WorkStation, Microsoft Hyper-V etc. Type 1 Hypervisors on the other hand have the virtualization layer directly running on the physical layer of the system, they are often colloquially known as "Bare-Metal Hypervisors". Operating within a layer of virtualization software, Oracle VirtualBox provides a platform for creating and managing virtual machines (VMs). VMs are self-contained instances of an operating system,

comprised of virtualized hardware components such as processors, memory, disks, and network interfaces. These VMs can be isolated from one another, simulating distinct physical systems, while sharing the underlying host's resources such as RAM, Processor CPUs, Storage as well as the networks (*What is a Virtual Machine? | VMware Glossary*, no date).

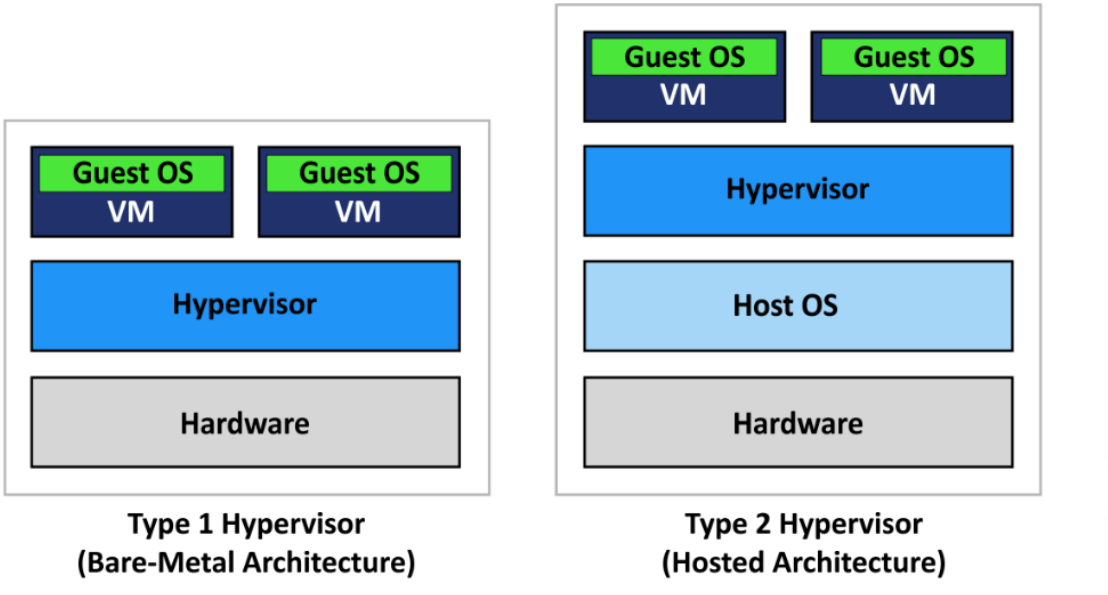

Fig.1 Type 1 vs Type 2 Hypervisors (*Hyper-V vs VirtualBox: In-Depth Comparison*, 2018)

The foundation of virtualization lies in the concept of abstraction, where the physical hardware is encapsulated and transformed into a manageable and distributable resource pool. This abstraction enables the creation of VMs that are entirely decoupled from the host hardware, allowing for improved resource allocation, efficient workload management and also enhanced system flexibility (*What Are Virtual Machines (VMs)?*, no date).
However, this virtualization landscape is not devoid of challenges. Sharing resources and information between VMs and the host OS introduces security risks, particularly in scenarios where shared resources are misconfigured or inadequately protected. These vulnerabilities can result in unauthorized access, data leakage, and even VM escape—wherein a VM gains access to the host system ('The Basics of Virtualization Security', no date).

To address these concerns, this research project delves into the domain of virtualization security, focusing specifically on Oracle VirtualBox. The project aims to analyze and address the vulnerabilities that arise from shared folder configurations and their potential to lead to VM escape scenarios (*Critical VMware Security Alert for Windows-Hosted VMware Workstation, VMware Player, and VMware ACE (1004034)*, 2014). By investigating these vulnerabilities, the project seeks to understand the risks associated with shared folders, explore their exploitation potential, and also to implement practical mitigation strategies. This is achieved through a combination of theoretical exploration, practical experimentation and finally solution implementation. This research project bridges the gap between theoretical vulnerabilities and tangible security measures. The insights gained contribute to the growing body of knowledge in virtualization security, offer guidance for practitioners, researchers as well as IT Administrators for organizations, and emphasize the importance of safeguarding virtualized environments from potential threats. In the following sections, we delve deeper into the technicalities of virtualization security within Oracle VirtualBox and the specifics of shared folder vulnerabilities and their mitigation.

Motivations

Rise of Security Concerns in Virtualization Environments: The increasing reliance on virtualization technologies, particularly opensource hypervisors like Oracle VirtualBox, has brought heightened attention to the security vulnerabilities inherent in such complex environments. Usually, educational institutions utilize free.

and opensource technologies such as VirtualBox for lab projects for universities and schools. As organizations adopt virtualization for their IT infrastructures, the potential risks associated with unauthorized code execution, VM escape, and data breaches become critical concerns (*5 common virtualization problems and howto solve them | TechTarget*, no date).

Dependence of Virtualization in Cloud Computing: Cloud computing heavily relies on virtualization to optimize resource utilization. Security vulnerabilities within virtualized environments could lead to not only individual system breaches but also effects across cloud infrastructures. Mitigating and resolving such vulnerabilities is pivotal to ensuring the integrity and confidentiality of cloud-hosted applications and data (*13Important Benefits of Virtualization in Cloud Computing*, no date).

Lack of Granular Access Control in Shared Folders: VirtualBox's shared folder functionality lacks fine-grained access control mechanisms. This gap poses a significant security challenge as shared folders can inadvertently expose sensitive data and allow unauthorized code execution between guest and host operating systems. Addressing this limitation becomes essential to ensure proper security measures are set in place (Ekrem, 2015).

Real world Implications of VM Escape: Successful VM escape attacks have real-world consequences, enabling attackers to gain unauthorized access to host systems and potentially compromise other virtual machines on the same hypervisor. As VM escape vulnerabilities can be used as stepping-stones for more advanced attacks, understanding, mitigating, and preventing such scenarios is of major importance (Constantin, 2015).

Gaps in Current Virtualization Security Knowledge: While virtualization security is a well-researched area, the specific focus on vulnerabilities stemming from shared folders in Oracle VirtualBox remains relatively unexplored. As virtualization technologies evolve, new vulnerabilities may emerge, necessitating updated security measures and practical solutions specific to the unique characteristics of each hypervisor (*Why you shouldn't use shared folders, shared clipboard and Drag'n'Drop*, no date).

Practical Application and Relevance: The project's outcomes directly impact practitioners, administrators, and researchers working with Oracle VirtualBox or similar virtualization solutions. By providing insights into vulnerabilities, proposing practical solutions, and emphasizing the importance of securing shared folder interactions, the project directly contributes to enhancing the security of virtualized environments.

Research Question

RQ1: What are the possible vulnerabilities in shared folder interactions between the guest virtual machine and host operating systems within a hypervisor?

This question focuses on identifying the security gaps that arise due to the shared folder feature and also identifying the current access controls, communication mechanisms, and potential unauthorized actions.

RQ2: Can unauthorized code execution be carried out via shared folders between a Guest VM and a Host OS?

This question delves into the technical aspects of exploiting shared folder vulnerabilities, exploring how a malicious guest OS program could leverage shared folders to execute unauthorized code on the host OS, leading to potential VM escape scenarios.

RQ3: What are the implications of Virtual Machine escape vulnerabilities and unauthorized code execution on the security posture of virtualized environments within a hypervisor?

This question examines the broader impact of vulnerabilities on virtualized environments, considering the potential risks, consequences, and real-world implications that unauthorized code execution could have on the overall security of the Virtualization Infrastructure.

RQ4: How can granular access control mechanisms be implemented to enhance the security of shared folder interactions in Oracle VirtualBox?

This question focuses on proposing solutions to resolve the identified vulnerabilities specifically in shared folder resources. It explores the possibility of solving granular access control mechanisms to ensure that sharedfolder interactions remain secure, limiting the potential for unauthorized actions.

RQ5: Can the usage of a type of security certificate be able to mitigate unauthorized code execution between guest and host operating systems in a hypervisor?

This question evaluates a proposed mitigation strategy, specifically the implementation of a security certificate to prevent unauthorized code execution. It assesses the degree to which the security certificate enhances the security posture of the virtualized environment and its interactions between a Guest OS and a Host OS.

Based on the above research questions, the following two critical points are to be addressed in this research project, which are the **security controls** and threats **against shared folder resources**. Given that the motivationof this project was directed towards a security concern for a business, for this project, the scope of the research will be focused on a scale down version of a lab setup that is running a Type 2 hypervisor with a virtual machine instance which replicates the scenario of a Cloud Based Virtual environment. However even if the scale of the study is limited and small, the results could be uniform even for a Cloud based environment or within an organization setup which is much larger in scale and size.

Potential Research Objectives

1. **Identification of Shared Folder Vulnerabilities:** To conduct an in-depth analysis of the vulnerabilities present in shared folder interactions between guest and host operating systems within a hypervisor specific to Oracle VirtualBox.

2. **Analysis of Virtual Machine Escape Scenarios**: To investigate potential scenarios where successful code execution from the guest VM to the host OS could lead to virtual machine escape, thereby compromising the host environment's security.

3. **Evaluation of Existing Security Measures**: By examining the default security features inbuilt in Oracle VirtualBox and assessment of their effectiveness in preventing unauthorized code execution and Virtual Machine escape through shared folders.

4. **Proposal of Novel Mitigation Strategies**: Development of innovative mitigation strategies to enhance shared folder security, focusing on granular access controls, authentication mechanisms, and secure communication protocols between the guest and host environments.

5. **Implementation and Test Security Measures**: Implement the proposed security measures within a controlled environment and assessment of their practicality, performance impact, and effectiveness in preventing unauthorized actions and Virtual Machine escape attempts.

The key goals of this research project are to understand the threat landscape, evaluate current security practices, identify the potential for enhancements to improve security, and to provide practical guidance to organizations leveraging virtualization technology either to adhere to a security framework guide or specific and targeted recommendations to ensure the security of the Virtualized environment. The research would produce specific, security controls to help secure hypervisor environments.

Hypothesis

"*A research hypothesis (or scientific hypothesis) is a statement about an expected relationship between variables, or explanation of an occurrence, which is clear, specific and testable*. (Jansen, 2020)"

Some of the potential hypothesis statements with regard to this research project are as follows.

Hypothesis 1: Vulnerabilities in the default security configurations of shared folders between guest and host operating systems in a hypervisor (in this case Oracle VirtualBox) can lead to unauthorized code execution on the host system, potentially enabling virtual machine escape from the Guest OS to the Host OS.

Hypothesis 2: Identification of Enhanced security measures implemented in Oracle VirtualBox, such as security certificates or access controls, can effectively mitigate the vulnerabilities associated with shared folder interactions, preventing unauthorized code-execution, and enhancing the overall virtualization security.

Hypothesis 3: The absence of granular access control and security configurations for shared folders in Oracle VirtualBox exposes virtual machines to significant security risks, potentially allowing malicious code execution and unauthorized data access.

Hypothesis 4: Comparative analysis of shared folder vulnerabilities across different virtualization platforms reveals that the issues observed in Oracle VirtualBox are representative of broader challenges within virtualized environments, emphasizing the importance of addressing shared folder security across the industry.

Hypothesis 5: By following to best practices for shared folder configuration by the vendors of the Hypervisors and maintaining a proactive security approach, organizations can effectively minimize the risks associated with unauthorized code execution and virtual machine escape in Oracle VirtualBox, creating a much more secure virtualization infrastructure.

These hypotheses cover a range of perspectives, from vulnerabilities and risks to potential solutions and industry-wide implications. Conducting research to investigate and validate these hypotheses will contribute valuable insights to the field of virtualization security.

2 Related Work

Virtualization technologies like hypervisors or Virtual Machine Monitors (VMM) underpin modern computing infrastructures and cloud environments, as per this paper from (Kumar and Kushwaha, 2018), it explicitly states that "Virtualization is the backbone of cloud technology". However, the risks of abstracting of physical resources between guest VMs and host systems also introduces various security risks that must be addressed as the paper from (Nyrkov *et al.*, 2018), supports that with virtualization technology and its abstraction of resource components, it greatly enforces the dependence of the virtualization in terms of software and thus increases the attack vectors from attackers to use it to their advantage to exploit the infrastructure. This literature review ingests and synthesis previous research papers in the domain of virtualization security, cloud security as well as hypervisor security that reviews various security issues along with their proposed mitigation techniques which in turn provides the motivation and inspiration to carry out this research thesis in the first place. Considerations to

2.1 Virtualization Security Overview

The surveyed papers establish virtualization can provide benefits like efficient resource utilization, flexibility, and scalability, however the paper from (Đorđević *et al.*, 2021) primarily focuses on the performance of the Guest OS in the hypervisor and Host OS which runs natively specifically to the file system performance. It goes to explain the benefits of the virtualization system such as isolation and efficient utilization of the resources, however it lacks when it is compared to that of a native operating system, this study validates that virtualization performance always will remain lower as compared to that of a native Operating system, however this is where Type 1 Hypervisors resolves the issue, by having the virtualization layer being as lightweight as possible and runs on a bare-metal setup, examples of this in commercial sense is VMWare ESXi, Microsoft Hyper-V(*What is ESXI | Bare Metal Hypervisor | ESX*, no date; *Hyper-V on Windows 10: An In-Depth Look*, no

date)As per the papers from(Kumar and Rathore, 2018) and (Wang *et al.*, 2019) both of them touch on points on the risks of uncontrolled shared folder access, lack of VM isolation in the virtualization layer and due to this vulnerabilities ranging from data leakage, unprotected shared memory as well as storage attack vectors can be exploited respectively .As per the paper from (Rastogi and Aggarwal, 2022) the hypervisors are a major target since its compromise gives control over all guest VMs that are hosted on the hypervisor once it is compromised as it can impact the entire infrastructure, as per this paper (Kapil, Mittal and Gangodkar, 2022), the authors explicitly mentions the type of attacks that can be used against a virtualized environment, such as VM Escape, shared resource isolation, analysis of multi-tenant environments with the lack of proper tenant isolation and also providing mitigation strategies such as sandboxing of VMs, proper Isolation and explicit access controls . Other risks include Virtual Machine escape exploits, isolation breaches between co-located VMs on the same host, and vulnerabilities in virtualized networking/storage as reviewed by the study from (Kadu, Jadhav and Pawar, 2022), both of those papers provide insights on the potential attack vectors as well as the mitigation strategies. Therefore, it can be seen that above papers, most of them suggests as part of the mitigation strategies to have proper access controls, VM isolation controls etc. Most of these papers that are considered in this literature reviews, give an idea of the potential attacks that are possible for the virtual machines on the hypervisors. They also provide insights on how to respond to those attacks. Some of these papers focus on the performance of hypervisors, but they do give an idea on the concept of virtualization and also introduce the risks associated within a virtualization infrastructure.

2.2 Shared Folder/Resources Security Issues

Several papers highlight shared folders or resources as a key threat vector in virtualized environments (Rastogi and Aggarwal, 2022), (Wang *et al.*, 2019), (Kumar and Rathore, 2018). Shared folders though facilitating useful Virtual Machine - Host filesystem interactions, most of them do not go into the review of the granular access controls of this shared folder and its permissions. As per the paper from (Alyas *et al.*, 2022), they go deep into the exploration into unique virtualization security risks such as VM Sprawl, lack of proper isolation between VMs via shared resources and also proposes a system to detect security risks in such a virtualized environment, though it does not provide a solution to mitigate or resolve such an attack from occurring, this paper focuses on the detection of the possible issues keeping in mind of the common Virtualization security risks. This paper from (Zhang *et al.*, 2018) focuses on the memory level attack vectors which is used to compromise VMs on a hypervisors, it focuses on “Neighbor VM attacks” which is similar to a VM Escape based attacks, wherein the attackers exploit the memory of the virtualized infrastructure to run malicious scripts to infect other VMs on the network or hypervisor. This paper proposes an internal VM detection system that relies on agents and signatures within the target guest virtual machines, but these are limited in their ability to counter advanced malware attacks. It focuses on a “VMI-based” detection involves using Virtual Machine Introspection (VMI) techniques to monitor the behavior of virtual machines from the hypervisor level and thwart any attempts to gain a higher-level privilege to exploit the infrastructure. As per this paper from (Avinash *et al.*, 2021), it goes more into the broad strokes of the Virtual Machine Exploits and the issues from the Hypervisor based attacks, VM based attacks and also the VM Image based attacks. As per the paper, risks in relation to that of the hypervisor, it seems that the most appropriate form of mitigating these risks is the usage of an Intrusion Detection System (IDS) which is basically a monitoring function that keeps checking the interactions between the systems. Another interesting finding from this paper is the exploration of risks to the VM image itself, though the proposed mitigation was regular system patches, but it.

touches on the topics of VM image integrity by enforcing correct access permissions for the images and their related snapshots.

As per this paper from (Li *et al.*, 2021), it goes to explore the concept of having a certificate-based authentication system specific to Virtualized system. Though this focuses on the interactions between the virtualized environment and their associated applications, the idea of integrating a security-based certificate system to ensure secure transmission of data between theOS and the application. This gave an idea to consider this form of authentication for the communication between the Guest OS to other VMs and also the host.

The paper appears to discuss the urgency of protecting virtual machines from sophisticated malware threats, especially for cloud service providers. This led to the curiosity to focus on one hypervisor and to consider Oracle VirtualBox for this project given its adoption in the market and is also an opensource software. Oracle VirtualBox does not have any form of fixed permissions that can ensure that shared folder interactions between the Guest OS to the Host OS can be controlled, this enables the options to execute malicious scripts in VMs to access sensitive host data or trigger privileged actions(Kumar and Rathore, 2018),(Wang *et al.*, 2019) such as code executions. But they do have only one single permission to enable read only for the file contents, when tested in the implementation, this setup seemed to be like to only view the contents of the file, but in reality, the purpose of a shared folder is to carryout transfer of files from one system to other in this case between a Guest OS and the native host system. Virtual Machine Escape to the Host OS as well as other Virtual machines in the hypervisors. Uncontrolled shared folder access combined with guest-host interconnectivity poses risks of Hypervisor/VM escape (Rastogi and Aggarwal, 2022), (Wang *et al.*, 2019), therefore identifying this as the security risk, consideration to delve deeper into this vulnerability and try exploiting it and verifying that this vulnerability can be exploited to interact with the host was developed. This realization is an important factor for this project, this is because, most users tend to utilize freeware and opensource software's such as Oracle VirtualBox for their development environments and in some cases even for production use cases. This software is very much capable of running production level applications and servers for businesses. Keeping this in mind, it was essential to investigate the extent of risks such as Virtual Machine Escape, Code injections etc. The chances of having these organizations utilize shared folder between the guest virtual machines and host OS can be reasonably high as even in development or production scenarios, there will be a point in time where file transfers between the Guest and Host will be a requirement. Though there are no official statistical figures to showcase this claim, it can be assumed that users in a business environment will have some level of shared folder access between the Host and the Guest.
After reviewing the above papers, the concept of virtual machine escape was identified as the ability to exit the virtual Guest OS environment and gain a higher privilege to execute commands or access other Virtual machines in the hypervisor or even the Host OS. Usually, this form of attack involves manipulating or attacking the physical level shared resources to achieve this, especially memory and the processor. By reviewing the study from those papers, an idea to explore the possibilities of replicating a VM escape via the shared folders was formed and was the primary motivation to proceed with the research in this domain (Lin *et al.*,2023). Though the papers that were referenced did not have a direct relevance in terms of an implementation of this project specifically for exploitation via shared folder, it did provide a basis and template to investigate the possibility of a virtual machine escape exploit and the mitigation to resolve such an issue.

2.3 Conclusion

In summary, this literature review establishes shared resources as a key virtualization security concern. Proposed mitigation techniques from most of the papers reviewed, emphasizes strictly on access controls, resource isolation, and securing the hypervisor by having a monitoring system in place. Combined adoption of these solutions can potentially close vulnerabilities introduced by indispensable VM-host sharing.

3 Research Methodology

Research Approach

This study employs an exploratory research approach to investigate vulnerabilities in virtualization security and the execution of code between guest and host systems in Oracle VirtualBox via shared folders. The project involves both practical demonstrations and theoretical analysis to uncover potential security gaps found in the Oracle VirtualBox Hypervisor. Based on the literature review of the papers mentioned above and identification of the possible attacks that can be used to cause a VM escape to occur via the shared resources, this project focuses on the utilization of the shared folder to act as a communication channel between the Guest OS and the Host OS. Identification of the current security controls enabled by default by the hypervisor, review of the file system permissions of the shared folder will be explored to ensure that no level of modification is being carried out to the default setup of the Hypervisor as well as the Guest OS setup.

1. **Setup Creation**: Development of a controlled environment with a Guest OS which is a Windows 10 Operating system using Oracle VirtualBox. Creation of a shared folder between the Guest OS and the Host OS is carried out by creating the shared folder on the Host OS which is Windows 11 and then mapping this shared folder to the Guest OS via the Hypervisor shared folder mapping settings by default.

2. **Code Execution**: In this section, a method to interact with the host Operating system from the Guest OS via the shared folder is kept as the objective. The second objective is to ensure that a communication pass through should take place wherein the trigger to execute something in this case was chosen to open an Excel application on the Host OS. Therefore, the objective was to make sure that the attack vector is very simple in terms of minimal scripts. The file types used were basic batch scripts and PowerShell scripts. The implementation is a three-step process where the Guest OS executes a batch script to generate a .txt file while the host OS has a listener PowerShell script which identifies the presence of this .txt file and then executes the code to open the required application on the host. The main point to be noted here is the reason as to why there is no security control to limit and write this .txt file from the guest OS onto this shared folder.

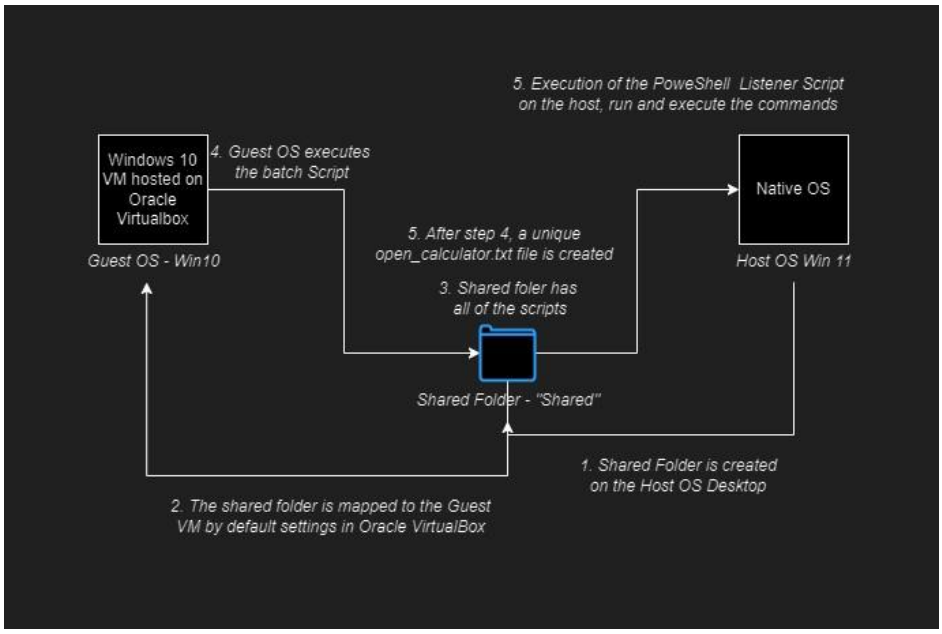

Fig. 2 Communication between Guest and Host OS

3. **Security Measures**: Implementing a security certificate-based solution on the Host OS to prevent unauthorized code execution. Within the listener script, there is a security check to ensure that with the presence of a specific security file in the shared folder, no level of communication should pass through between the Guest OS and the Host OS. This logic is embedded in the initial PowerShell script which displays the code execution initially.

4. **Logs and Observations**: Identification of the current level of security policies for the shared folder will be identified in this section, default configuration and access control will be reviewed. Utilization of process explorer to identify the Guest OS behavior at the time of the execution will be identified and discussed.

5. **Performance Metrics**: Measure resource utilization and performance impact on both guest and host systems during code execution. This is also identified via Process Explorer.

6. **Controlled Exploitation:** Introduce controlled code execution attempts from the Guest OS to the Host OS, observing potential outcomes. This section focuses on the addition of the security file check and the stoppage of the code execution.

Results and Findings

To present the findings of the experiments, showcasing the vulnerabilities discovered, potential risks, and the impact of the security certificate-based solution. Quantify the effectiveness of the security measure in preventing unauthorized code execution.

4 Design Specification

The design specification outlines the technical aspects of investigating a shared folder interaction between a Guest OS and a Host OS in Oracle VirtualBox. The goal of this study is to prevent unauthorized code execution while enabling controlled communication between the two operating systems.

Architecture

The project architecture consists of the following components:

1. **Guest OS:** A virtual machine running on Oracle VirtualBox, representing the Guest OS which in this case is a Windows 10 VM.

2. **Host OS:** The physical machine hosting the hypervisor and the Guest OS, which in this case is a Windows 11 Operating system.

3. **Shared Folder:** A folder on the Host OS which is located on the Desktop is mapped to the Guest OS as per the default settings from the Hypervisor – Oracle VirtualBox, enabling communication.

4. **Security Certificate**: A certificate required for executing commands on the Host OS triggered from the Guest OS which in this case is an empty .txt file, the important factor of this is the name of the file which will be embedded in the logic of the listener script such that, only in the presence of this file, the communication should not take place and this acts as a stoppage for the communication.

5. **Listening Script**: A PowerShell script running on the Host OS to monitor and validate commands from the Guest OS as well as checking for the security file to ensure that the code should not be executed via the Guest OS.

6. **Shared Folder Security:** The shared folder interaction is designed to ensure security and prevent unauthorized code execution:

7. **Access Control:** The Host OS enforces access controls on the shared folder, allowing only authorized users or groups to access and modify files. Another point to be noted is no modification of the access controls is carried out. And also, since there is no connection between the users and groups between the Host OS and the Guest OS, ideally, the Guest OS shouldn't have any form of explicit permission to write into this folder.

8. **Granular Permissions:** On the Guest OS, there is no form of control on the permission on this shared folder, since this folder was created in the Host OS. Secondly, there is no form of shared folder access control at the time of mapping this shared folder on the hypervisors. Therefore, this is to be considered as a lack of security control from the vendor of the VirtualBox, which in this case is Oracle.

Security Certificate Mechanism

The security certificate mechanism enhances security in the following ways:

Authorization: To execute a command on the Host OS, the listener script logic must check for a security certificate signed by a trusted authority in an ideal scenario or it can be also carried out by a special cryptographic key exchange, but in this case, just the placement of the security file in the shared folder is only carried out. But in this case, just to demonstrate the possibility of a security check, a security file was created and manually placed into the shared folder.

Certificate Validation: The listening script on the Host OS verifies the authenticity of the security certificate before executing the command, which in this case is to check the presence of it or not.

Communication Flow

The interaction between the Guest OS and Host OS follows these steps:

Guest OS Action: The Guest OS generates a .txt file along with a command request to output the status of its execution.

Shared Folder: The security certificate and generated open_calculator.txt file from the Guest OS is saved in the shared folder, when the batch script is executed by the Guest OS VM.

Listening Script: The listening script on the Host OS detects the presence of the security certificate as well as identifies the generated script, after which, if there is no security certificate present, then the code executes and the excel application opens, however if the security script is present, then nothing takes place.

Mitigation of VM Escape Vulnerabilities

By enforcing security certificates and validating commands, the project mitigates VM escape vulnerabilities that could arise from unauthorized Guest OS actions. The security certificate mechanism ensures that only authorized actions are executed on the Host OS in an ideal scenario, but in this case, in the presence of the security certificate the application on the Host OS would not execute.

5 Implementation

Outputs Produced

Security Certificate Validation: The security certificate validation is a security check which is integrated in the Listener script in PowerShell to ensure if the security certificate is available then no form of code execution should be taking place, irrespective of whatever .txt file is being created to prompt the initiation of opening any application on the Host Operating System.

Listening Script Output: The listening script on the Host OS will generate output logs indicating successful execution of authorized commands triggered by valid security.

certificates and will be continuously monitoring the shared folder as well as validating the security check.

Tools and Languages

Virtualization Platform: Oracle VirtualBox with the latest version is used for hosting both the Guest and Host OS.

Scripting Languages: PowerShell scripting language is utilized for developing scripts on the Host OS and batch scripting is used in the Guest OS to initiate the temporary trigger .txt file.

Text Editors: Text editors such as MS Notepad is used for writing and editing scripts.

Implementation Steps

Development of listener script via PowerShell (Host OS):

A basic script that has been created in two stages, in the first stage there is no security check as the intention was demonstrate the vulnerability of code execution based on the prompt generated open_calculator.txt file by the Guest OS. Therefore, the initial objective was to create a listener script which checks and monitors the shared folder in search of a specific file via its name. Once this file is found and confirmed then the code to open the relevant application takes place, which in this case is excel.exe. This works for calculator application and any other .exe file provided the relevant path to the file is provided.

Development of Guest OS Batch Script

This batch script is a basic script to echo out the log that the prompt to open the application is carried out as well as the generation of the temporary file .txt onto the shared folder. The monitor script automatically removes this file once the listener script process is stopped. This is done so that, the document does not remain and continues to execute the code on the Host OS. Therefore, the only major output from this script is to ensure that the open_calculator.txt file is being generated in the correct Shared Folder.

Secure Listener Script

This script is a modified version of the Listener Script which has a logic where in it monitors the shared folder as well as identifies the presence of the security certificate.txt file which has no content in it, rather the check just verifies the presence of this file by its name and if present it is tasked to block the execution of the code.

6 Evaluation

The evaluation phase of this project aims to analyze the outcomes and findings of the implemented solution, which addresses the vulnerabilities related to VM Escape, code injection, and shared folder security within Oracle VirtualBox. Key results will be presented, highlighting the effectiveness of the security measures implemented to prevent unauthorized code execution and mitigate VM escape risks.

Scripting and VM Escape Analysis

The evaluation delves into the specific scenarios involving scripting and VM escape. It will assess the ability of the Guest OS to communicate with the Host OS through shared folders, execute code, and potentially exploit VM escape vulnerabilities. The evaluation will identify instances of unauthorized actions and code executions to determine the potential security risks.

Security Mechanisms Effectiveness

The evaluation will comprehensively analyze the effectiveness of the security mechanisms integrated into the solution. This includes the security certificate requirement to validate command execution requests from the Guest OS. Success rates of security certificate validation and the frequency of unauthorized code executions will be evaluated to gauge the efficacy of the security measures. The success rate is 100 percent as it stops the execution of the code.

Implications and Significance

The significance of identifying and mitigating vulnerabilities that could lead to VM escape is a critical concern in virtualization security. Academic and practical implications will be highlighted, emphasizing the importance of securing shared folders and preventing unauthorized code execution.

7 Conclusion and Future Work

In the field of virtualization security, this research project started out on a comprehensive exploration of vulnerabilities within Oracle VirtualBox, focusing on scripting interactions, VM escape risks, and risks to shared folder security. The project not only identified potential threats but also proposed and implemented a novel security mechanism to address these concerns. By engaging in practical experimentation, analysis, and evaluation, this project provided valuable insights into safeguarding virtualized environments and preventing unauthorized code execution. It is also important to note that no changes to the Hypervisor and the latest versions of the software was used to demonstrate.

Achievements and Contributions

The project began by unveiling the foundational concepts of virtualization security, exposing the risks posed by shared folders and the potential chances for Virtual Machine escape.
Leveraging Oracle VirtualBox as the hypervisor of choice, a solution was crafted to mitigate these vulnerabilities. The implementation of a security certificate requirement introduced a vital layer of defense, ensuring that only authorized actions originating from the Guest OS could impact the Host OS. Through rigorous testing and analysis, the project demonstrated the effectiveness of the proposed security measure in resolving unauthorized code execution and enhancing overall virtualization security.

Significance

The project's findings hold implications for both the academic and practitioner communities in business environments. The study underscored the critical importance of securing shared folder communications and mitigating the risks of VM escape, a concern that has far-reaching consequences for virtualized environments. By showcasing the potential security gaps and vulnerabilities that can arise, the project emphasizes the necessity of proactive measures to protect virtualized systems.

Future Research Directions

While this project has made significant strides in addressing virtualization security concerns, there remain several promising avenues for future research:

Enhanced Security Mechanisms: Further refinement of the security certificate approach can be explored, ensuring even more robust authorization mechanisms for code execution requests.

Hypervisor Diversity: Extending the study to encompass a broader range of hypervisor environments will provide insights into vulnerabilities specific to different virtualization platforms.

Advanced Threat Scenarios: Investigating more intricate threat scenarios, such as memory-based attacks and privilege escalation attempts, will offer a deeper understanding of potential exploitation vectors.

Automated Security Tools: Developing automated security tools that dynamically monitor and respond to unauthorized actions between Guest and Host OS can provide real-time protection.

Industry Collaboration: Collaborating with virtualization software vendors to integrate enhanced security features at the hypervisor level can contribute to more secure virtualized environments.

Conclusion

In conclusion, this research project has addressed a critical concern in the field of virtualization security by proposing a solution to prevent unauthorized code execution and mitigate VM escape vulnerabilities. The combination of theoretical analysis, practical implementation, and rigorous evaluation has contributed to the body of knowledge surrounding virtualization security. By bridging the gap between theoretical vulnerabilities and real-world solutions, this project showcases the importance of securing virtualized systems in the modern computing landscape.

As the field of virtualization continues to evolve, the lessons learned from this project pave the way for a safer and more resilient virtualized ecosystem. By continually refining security practices and exploring emerging threats, researchers and practitioners can collectively advance the state of virtualization security and build a more secure digital future.

References

1.1.1. Brief History of Virtualization (no date). Available at: https://docs.oracle.com/cd/E26996_01/E18549/html/VMUSG1010.html (Accessed: 11 August 2023).

5 Benefits of Virtualization (2021). Available at: https://www.ibm.com/cloud/blog/5-benefits-of-virtualization (Accessed: 14 April 2023).

5 common virtualization problems and how to solve them | TechTarget (no date) *IT Operations*. Available at: https://www.techtarget.com/searchitoperations/feature/5-common-virtualization-problems-and-how-to-solve-them (Accessed: 13 August 2023).

13 Important Benefits of Virtualization in Cloud Computing (no date). Available at: https://www.knowledgehut.com/blog/cloud-computing/benefits-of-virtualization-in-cloud-computing (Accessed: 13 August 2023).

Administrator. (2013) 'Common Virtualization Vulnerabilities and How to Mitigate Risks', *Penetration Testing Lab*, 25 February. Available at: https://pentestlab.blog/2013/02/25/common-virtualization-vulnerabilities-and-how-to-mitigate-risks/ (Accessed: 13 August 2023).

Alyas, T. *et al.* (2022) 'Security Analysis for Virtual Machine Allocation in Cloud Computing', in *2022 International Conference on Cyber Resilience (ICCR)*. *2022 International Conference on Cyber Resilience (ICCR)*, pp. 1–9. Available at: https://doi.org/10.1109/ICCR56254.2022.9996066.

Avinash, J. *et al.* (2021) 'TOUR TOWARDS THE SECURITY CHALLENGES OF VIRTUALIZATION IN CLOUD COMPUTING: A SURVEY', in *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*. *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 771–776. Available at: https://doi.org/10.1109/ICOEI51242.2021.9452879.

Constantin, L. (2015) *Critical VM escape vulnerability impacts business systems, data centers*, *Computerworld*. Available at: https://www.computerworld.com/article/2922215/critical-vm-escape-vulnerability-impacts-business-systems-data-centers.html (Accessed: 13 August 2023).

Critical VMware Security Alert for Windows-Hosted VMware Workstation, VMware Player, and VMware ACE (1004034) (2014). Available at: https://kb.vmware.com/s/article/1004034?lang=en_US (Accessed: 13 August 2023).

Đorđević, B. *et al.* (2021) 'Performance comparison of native host and hyper-based virtualization VirtualBox', in *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*. *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–4. Available at: https://doi.org/10.1109/INFOTEH51037.2021.9400684.

Ekrem (2015) 'In VMs, do shared folders reduce security effectiveness?', *Information Security Stack Exchange*. Available at: https://security.stackexchange.com/q/102989 (Accessed: 13 August 2023).

Hyper-V on Windows 10: An In-Depth Look (no date) *Perception Point*. Available at: https://perception-point.io/guides/virtual-browser/hyper-v-on-windows-10-an-in-depth-look/ (Accessed: 13 August 2023).

Hyper-V vs VirtualBox: In-Depth Comparison (2018) *Nakivo*. Available at: https://www.nakivo.com/blog/hyper-v-virtualbox-one-choose-infrastructure/ (Accessed: 13 August 2023).

Jansen, D. (2020) ‘What Is A Research Hypothesis? A Simple Definition’, *Grad Coach*, 8 June. Available at: https://gradcoach.com/what-is-a-research-hypothesis-or-scientific-hypothesis/ (Accessed: 31 July 2023).

Kadu, N.B., Jadhav, P. and Pawar, S. (2022) ‘Virtual Machine Migration Techniques, Security Threats and Vulnerabilities’, in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*. *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 444–449. Available at: https://doi.org/10.1109/IC3I56241.2022.10072960.

Kapil, D., Mittal, V. and Gangodkar, D.P. (2022) ‘Virtualization and Nested Virtualization Technology: Concept, Architecture and Attack Vector Model’, in *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*. *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, pp. 349–354. Available at: https://doi.org/10.1109/CISES54857.2022.9844347.

Kumar, S. and Kushwaha, A.S. (2018) ‘Virtualization Backbone of Cloud Computing - Analysis’, in *2018 4th International Conference on Computing Sciences (ICCS)*. *2018 4th International Conference on Computing Sciences (ICCS)*, pp. 35–39. Available at: https://doi.org/10.1109/ICCS.2018.00012.

Kumar, V. and Rathore, R.S. (2018) ‘Security Issues with Virtualization in Cloud Computing’, in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*. *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 487–491. Available at: https://doi.org/10.1109/ICACCCN.2018.8748405.

Li, B. *et al.* (2021) ‘Locally-Centralized Certificate Validation and its Application in Desktop Virtualization Systems’, *IEEE Transactions on Information Forensics and Security*, 16, pp. 1380–1395. Available at: https://doi.org/10.1109/TIFS.2020.3035265.

Lin, K. *et al.* (2023) ‘HyperPS: A Virtual-Machine Memory Protection Approach Through Hypervisor’s Privilege Separation’, *IEEE Transactions on Dependable and Secure Computing*, 20(4), pp. 2925–2938. Available at: https://doi.org/10.1109/TDSC.2022.3200206.

Misconfigured Cloud Services Pose High Security Risks for Organizations - Wiadomości bezpieczeństwa (no date). Available at: https://www.trendmicro.com/vinfo/pl/security/news/virtualization-and-cloud/-misconfigured-cloud-services-pose-high-security-risks-for-organizations (Accessed: 13 August 2023).

Nyrkov, A.P. *et al.* (2018) ‘Analysis of platform vulnerabilities for the virtualization process’, in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 94–97. Available at: https://doi.org/10.1109/EIConRus.2018.8317038.

Rastogi, R. and Aggarwal, N. (2022) ‘A Review on Virtualization and Cloud Security’, in *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*. *2022 2nd International Conference on Innovative Practices in Technology and*

Management (ICIPTM), pp. 162–166. Available at: https://doi.org/10.1109/ICIPTM54933.2022.9754172.

'The Basics of Virtualization Security' (no date) *https://blog.netwrix.com/*. Available at: https://blog.netwrix.com/2020/01/09/virtualization-security/ (Accessed: 15 April 2023).

Wang, X. *et al.* (2019) 'Design and Implementation of SecPod, A Framework for Virtualization-Based Security Systems', *IEEE Transactions on Dependable and Secure Computing*, 16(1), pp. 44–57. Available at: https://doi.org/10.1109/TDSC.2017.2675991.

What Are Virtual Machines (VMs)? (no date) *Kong Inc.* Available at: https://konghq.com/learning-center/service-mesh/virtual-machines (Accessed: 13 August 2023).

What is a Virtual Machine? | VMware Glossary (no date) *VMware*. Available at: https://www.vmware.com/topics/glossary/content/virtual-machine.html (Accessed: 13 August 2023).

What is ESXI | Bare Metal Hypervisor | ESX (no date) *VMware*. Available at: https://www.vmware.com/products/esxi-and-esx.html (Accessed: 13 August 2023).

Why you shouldn't use shared folders, shared clipboard and Drag'n'Drop (no date). Available at: https://book.cyberyozh.com/why-you-shouldnt-use-shared-folders-shared-clipboard-and-dragndrop/ (Accessed: 13 August 2023).

Zhang, S. *et al.* (2018) 'Secure Virtualization Environment Based on Advanced Memory Introspection', *Security and Communication Networks*, 2018, pp. 1–16. Available at: https://doi.org/10.1155/2018/9410278.