Journal of Global Business Insights

Volume 6 | Issue 2 Article 2

September 2021

Enterprise environment modeling for penetration testing on the OpenStack virtualization platform

Vincent Karovic Jr.
Comenius University, vincent.karovic2@fm.uniba.sk

Jakub Bartalos
Comenius University, jakub.bartalos@fm.uniba.sk

Vincent Karovic
Comenius University, vincent.karovic2@fm.uniba.sk

See next page for additional authors

Recommended Citation

Karovic, V., Bartalos, J., Karovic, V., & Gregus, M. (2021). Enterprise environment modeling for penetration testing on the OpenStack virtualization platform. *Journal of Global Business Insights, 6*(2), 117-140. https://www.doi.org/10.5038/2640-6489.6.2.1152

Enterprise environment modeling for penetration testing on the OpenStack virtualization platform

Authors

Vincent Karovic Jr., Jakub Bartalos, Vincent Karovic, and Michal Gregus

Corresponding Author

Vincent Karovič Jr., Department of Information Systems, Faculty of Management, Comenius University, Odbojárov 10, 81499 Bratislava, Slovakia

Abstract

The article presents the design of a model environment for penetration testing of an organization using virtualization. The need for this model was based on the constantly increasing requirements for the security of information systems, both in legal terms and in accordance with international security standards. The model was created based on a specific team from the unnamed company. The virtual working environment offered the same functions as the physical environment. The virtual working environment was created in OpenStack and tested with a Linux distribution Kali Linux. We demonstrated that the virtual environment is functional and its security testable. Virtualizing the work environment simplified the organization's security testing, increased resource efficiency, and reduced the total cost of ownership of certain devices.

Keywords

network modelling, information security, security testing

Revisions

Submission date: Aug. 7, 2020; 1st Revision: Sep. 23, 2020; 2nd Revision: Jan. 22, 2021; 3rd Revision: Mar. 22, 2021; Acceptance: May 5, 2021

Enterprise Environment Modeling for Penetration Testing on the OpenStack Virtualization Platform

Vincent Karovič Jr.[1], Jakub Bartaloš[2], Vincent Karovič[3], and Michal Greguš[4]

Department of Information Systems
Faculty of Management
Comenius University, Bratislava, Slovakia
[1]vincent.karovic2@fm.uniba.sk
[2]jakub.bartalos@fm.uniba.sk
[3]vincent.karovic@fm.uniba.sk
[4]michal.gregus@fm.uniba.sk

Abstract

The article presents the design of a model environment for penetration testing of an organization using virtualization. The need for this model was based on the constantly increasing requirements for the security of information systems, both in legal terms and in accordance with international security standards. The model was created based on a specific team from the unnamed company. The virtual working environment offered the same functions as the physical environment. The virtual working environment was created in OpenStack and tested with a Linux distribution Kali Linux. We demonstrated that the virtual environment is functional and its security testable. Virtualizing the work environment simplified the organization's security testing, increased resource efficiency, and reduced the total cost of ownership of certain devices.

Keywords: network modeling, information security, security testing

Introduction

Information security is a topical issue currently addressed by many organizations. Proper information is one of the most important assets for managers. However, as the volume of information increases, so does the need to protect it. Companies and governments are aware of this. On 25 May 2018, the European Union's Personal Data Protection Regulation emerged, regulating the way organizations process and manage personal data (Wahl, 2020). Companies may be fined up to 20 million euros or 4% of their annual turnover if data leakage or serious misconduct occur (Intersoft Consulting, n.d.). However, the regulation is only one of many reasons companies should pay sufficient attention to information security.

Each company has its own physical infrastructure design and configuration set up. The differences are in the technologies used, network topologies, computational power, storage sizes, physical hardware layout and, above all, the purpose for which the overall infrastructure is used. At present, these differences represent a huge challenge to ensure security for organizations. The security of the information system must be constantly updated as new threats emerge every day. However, security

solutions can be costly or detrimental to many organizations who may lose time and productivity due to system downtime from system testing (Marget, 2021).

OpenStack technology brings a new perspective to the issue, enabling organizations to move from the physical work environment to a virtual environment (Karande et al., 2015). The virtual work environment provides the same capabilities as the physical environment, resulting in two identical work environments with the same infrastructure, workstations, and systems. This allows the virtual environment to be tested independently of the physical environment. The main advantage of virtualization modeling is the separation of the physical environment from operating systems and their installation needs for each application. This brings great flexibility with existing hardware. There is also room to model different topologies and solutions, which would take a long time if implemented physically (Oracle, n.d.).

The main objective of this work was to create an environment model to test the security of organizations through virtualization. To achieve this objective, we address the importance of information system security from a business and legal point of view, explain the concept of virtualization and build and test a virtual work environment. After explaining the theoretical bases, the experiment was designed, built, and tested in a virtual environment. The input data prior to the experiment was obtained by observing the environment of an unnamed company. The result is a functional and virtualized workspace whose security can be tested. The output data were interpreted during the discussion and are included in the recommendation of this work.

To meet our main objective, we identified and met the following partial objectives: defined basic terms and content of the terms, defined virtualization, defined software needed to model and test security, analyzed the current situation in the organization, created an organization's work environment model, tested the security of the virtual workspace, identified additional benefits of desktop virtualization, and offered conclusions and recommendations.

Literature Review

This section explains the related work of the theoretical base important for modeling an environment to test the security of an organization using virtualization. The review covers the importance of quality information for the manager, the importance of protecting information systems, and the theoretical background for virtualization modeling.

Manager and Information

A significant part of the manager's activities in terms of content and time of consumption is working with information to motivate, guide, organize, and control people (Hobart & Schiffman, 2000). For effective management, the manager needs a filtered minimum of relevant data and information crucial for decision making and management of the object (Sebetci, 2020).

As management demands increase and information generation increases, the discrepancy between managing (processing) available information and available time increases. Therefore, a manager must have enough relevant and quality information. Often, a manager is inundated with unnecessary information that takes up time, obscures the image, and does not contribute to improving the quality of management. Such information is called noise of information processes. Depending on the manager's functions in the management system, targeted information selection is required (Molnár et al., 2014).

For quality of management, however, a manager requires more than sufficient quality information. Management must also have quality methods and efficient means of processing them. It is equally important to know the optimal level of quantity (e.g., a threshold above which the quality of management does not increase, but actually deteriorates.) In this context, gate keeping—filtering information for the manager to avoid an excess of irrelevant and missing key information—has emerged in the literature. The manager needs information to fulfill their functions in the management system (Hobart & Schiffman, 2000).

Security of the Information System

The security of an information system in an organization should not be the concern of a few people, but of all employees of the organization. However, it is unrealistic to expect or require every worker to have a high level of expertise in such a specific area. Acquiring specific information is necessary but not enough to when the information is constantly updated. This knowledge such as the emergence of new threats, new methods of intrusion or bypassing security barriers, and the discovery of gaps in established programs.

Therefore, in some organizations, the responsibility for information system security is assumed by the system administrator. However, this solution cannot be considered satisfactory. The system administrator has sufficient work to ensure the operation of the system, maintenance of equipment, and troubleshooting for users. Little time remains to monitor information security developments. In terms of basic security principles, such a solution is equally impractical because an individual who accumulates high privileges may manipulate the system, developing powers to design, implement, install, and maintain security measures and respond to suspicions of unauthorized activity in the system. The result is a high risk of *information control* of the organization by a single individual whose activity is essentially uncontrollable (Blokdyk, 2020b).

To ensure an adequate level of security of the information system in the long term, assigning a separate and specialized information security unit is appropriate, especially for large organizations. The size of such a unit is largely determined by the size of the organization and the needs to ensure the information system. The level of internal hierarchy to which this unit is assigned will indicate not only the importance it attaches to information system security in the organization, but also the competence of the unit and the potential effectiveness of the work entrusted to it. The workload of a specialized unit varies from one organization to another depending on the needs and requirements of a particular organization, but it should include at least the following activities (Blokdyk, 2020b; Kim & Solomon, 2016):

- Serves as a specialized advisory body to senior management on security and system reliability issues
- Elaborates the concept of information system security and coordinates its implementation across the whole organization
- Promotes and coordinates the training of the organization’s staff in information security
- Develops standards, internal regulations, and procedures directly related to the secure operation of the information system and provides expert opinion on standards, internal regulations, and procedures from other departments in terms of their impact on the security of the information system
- Serves as a central point for the organization’s staff on information system security issues

- Systematically acquires and evaluates information on the status and development of methods and means for securing information systems, their advantages, disadvantages, and limitations
- Systematically obtains and evaluates information on methods and means used or used for unauthorized intrusion through existing security barriers
- Organizes its own control activities, checks compliance with standards, regulations, and procedures designed to increase and maintain the security of the information system; thoroughly investigates discovered security incidents; and transfers the general knowledge into the update of existing security measures (Blokdyk, 2020b; Kim & Solomon, 2016).

Chief Information Security Officer (CISO)

The CISO is a person directly subordinate to the Chief Executive Officer. They work at the same level with the Chief Information Officer but should be given special powers in case of a crisis situation. Only in very large organizations does a separate information technology (IT) security department exist—hence, most of the time, the security director is also the superior IT department (Karanja, 2017).

The main task of the CISO is to analyze the current situation in the organization and propose improvements. To this end, the CISO creates the organization's security policy and, through these powers, oversees their implementation into internal organizational practice. The CISO ensures ongoing security policy updates according to the changing requirements of employees and management. In the event of a crisis, the CISO is responsible for resolving problems as quickly and effectively as possible. Qualified, the CISO should be at the same level as the Chief Information Officer. They should have sufficient managerial skills and abilities such as leading a team of people in both normal and crisis situations and knowledge of both information technology and information system security. The CISO should also be familiar with the organizational structure and internal processes (Allen, 2019).

Security Policy

Implementation of the security policy is only part of the process. The correctness of the implementation needs to be checked periodically to avoid intentional or unintentional human errors. Emergency plans are another part of the security policy. They set out specific steps to take for specific types of incidents. Their functionality should also be checked at regular intervals (Ofori et al., 2020). Security policy should not remain a fixed document. The environment of the information system changes over time. New threats and new assets must be protected. To make enforcement of security measures easier, company management should be familiar with the full policy (Allen, 2019).

Self-Assessment Information Security Environment

Information security is a topic that organizations approach differently. Management is faced with many decisions about how to deal with it, how much to invest in it, and so on. These decisions rationally rely on a mix of inputs, beginning with the organizational strategy and the requirements of the owners or shareholders, and ending with specific problems addressed by either IT staff or security experts. Self-assessment plays an important role in the field of information security and can facilitate a significant number of decisions (Kim & Solomon, 2016). Many methods and automated tools for

self-assessment of information security exist. They differ mainly in their focus, content, or form (Allen, 2019; Hwang et al., 2017).

Information relatively easy to learn through self-assessment gives the organization a clear idea of the level of information security in each area and helps prioritize its solution. Equally important is a manager's need to argue for or justify a budget for security or to launch security projects. If the company decides to cooperate with an external company for an information security solution, the manager can use the self-assessment to define the content and scope of the basic services in the preparation of the tender (Allen, 2019).

Legislation and Standards

This section explains the importance of addressing information security, its benefits for the organization, and possible sanctions an organization may receive from security incidents.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the legislative guideline for the processing of personal data applicable to all countries in the European Union. The Regulation is mandatory for all members of the European Union, but selected areas can be further regulated by individual states (for example, the level of sanctions based on infringements; Hoofnagle et al., 2019).

The General Data Protection Regulation governs the way organizations process and manage personal data. In effect from 25 May 2018 and applicable to all businesses and organizations (e.g., hospitals, public administrations, etc.), the Regulation represents the biggest change in data protection rules in the European Union in the last 20 years. The Regulation presents a new opportunity for organizations to improve consumer confidence through the management of personal data. Organizations that fail to adequately protect an individual's personal data risk loses consumer confidence (European Commission, 2018).

The Regulation shall apply to the Organization if:

- The organization processes personal data and has its registered office in the European Union, regardless of where the data processing actually takes place
- The organization is based outside the European Union but offers or monitors goods or services to individuals within the European Union (Černá & Sieber, 2018)

Personal Data

The Regulation clarifies the concept of personal data in such a way that different types of online personal identifiers (cookies, IP address) and other electronic identifiers (location data, RFID technologies) are also considered to be personal data. Personal data that have been pseudonymized, but which can be used to re-identify a person always fall within the scope of the Data Protection Regulation. Pseudonymized data are encrypted data which do not directly identify the person, but which, once decrypted using a suitable key, become identifiable personal data again. Personal data which have been irrevocably anonymized in such a way that is the data are no longer possible to identify an individual within the Regulation are no longer considered personal data (Fuster, 2014).

Obligations of the Organization Under the Data Protection Regulation

The regulation applies strict rules on consent to the processing of personal data. The purpose of these rules is to ensure that the individual understands what they agree to. Consent should be given freely, and the individual should be clearly and unequivocally informed of what consent is given. The Regulation includes a number of obligations that organizations must comply with to protect an individual's right to control their own personal data:

If the processing of personal data is based on consent or under contract, an individual may request the return or transfer of personal data to another company. This is known as the right to transfer personal data. The data should be provided in a commonly used and computer-readable format (Černá & Sieber, 2018; European Commission, 2018).

Security breaches occur when personal data for which an organization is responsible is disclosed, whether accidentally or illegally, to an unauthorized recipient, or temporarily unavailable or altered. If a breach of security occurs and this breach constitutes a risk to the rights of the data subjects, the organization shall notify the breach to the supervisory authority within 72 hours of the breach being identified. Depending on how high the risk of disruption poses to the persons concerned, the organization may be required to inform all individuals concerned by the disruption (European Commission, 2018).

Penalties

Failure to comply with the Data Protection Regulation may lead to significant fines of up to EUR 20 million or 4% of the company's annual turnover, whichever is greater. The supervisory authority may additionally impose remedies such as an order to terminate the processing of personal data. For most organizations, GDPR requires significant changes in many parts of the organization; unfortunately, many small and medium-sized enterprises (SMEs) do not have resources or knowledge to manage this by themselves. Noncompliance may risk expensive penalties (Brodin, 2019; Zetoony, 2019).

Figure 1. Notice, Reprimand, and Suspension of Processing and Fines

Source: European Commission, 2018)

Information Security Management System (ISMS) Standards

The International Organization for Standardization (ISO) supports an expert committee dedicated to the development of international standards for information security management systems, otherwise known as the ISMS standards. These standards represent a model to follow when implementing and operating a management system within an organization. This model combines features agreed upon by experts and are considered the most advanced in the field.

ISMS compliance allows organizations to develop and implement a security management system for their information assets, including financial information, intellectual property, employee information, or information, entrusted to them by customers or third parties. These standards can also be used to prepare an independent assessment of the information security management system (Zetoony, 2019).

ISMS standards consist of policies, procedures, guidelines, and related activities and resources managed by the company to protect information assets. ISMS contains a systematic approach to the implementation, operation, monitoring, control, maintenance, and improvement of the organization's information security. It is based on risk assessment and the degree of avoidance of organizational uncertainty and is designed to effectively manage and eliminate risks. The analysis of the requirements for the protection of information assets and the application of appropriate management elements to ensure the protection of information assets contribute to the successful implementation of ISMS (Brodin, 2019). ISMS is for professionals who lead or participate in the creation, implementation, maintenance, and continuous improvement of one or more information security management system processes (Calder & Watkins, 2019; ISO, 2018).

Cybersecurity

Cybersecurity refers to the ability of any electronic communications network, electronic information, or control system to withstand reliability to accidental events or malicious activities, to a certain degree, that may negatively affect the authenticity, integrity, availability, or confidentiality of stored, processed, or transmitted data and services. provided through a network, information, or management system; and thereby disrupt or adversely affect the functionality of a particular critical infrastructure sector, namely one of the basic security areas of the functioning of the state (Kaczor & Kryvinska, 2013).

At the national level, cybersecurity is a system of continuous and planned improvements of legal, political, security, economic, defense, and educational awareness which also includes increasing the effectiveness of adopted and applied technical-organizational risk management measures in cyberspace to transform it into a trusted environment that enable the safe functioning of social and economic processes while ensuring an acceptable level of risk in cyberspace (European Commission, 2019).

Cybersecurity threats are diverse. The targets of the attacks are found not only in the state apparatus or military sphere, but also in the economic, environmental, and social sectors. Cybersecurity has unambiguous military implications—the most advanced technologies being used primarily by the armed forces which rely on information and communication technologies. In addition to the direct military security threats arising from the possibility that military systems, or classified information, would come under enemy control, one can also identify indirect and non-military cybersecurity threats. These relate to the aforementioned non-military sectors, specifically the energy, financial, and transport infrastructure of the state. In general, cyber threats can be divided into four categories:

- State and state-sponsored attacks
- Ideological and political extremism
- Organized crime
- Individual crime (Diogenes & Ozkaya, 2019)

Existing Systems

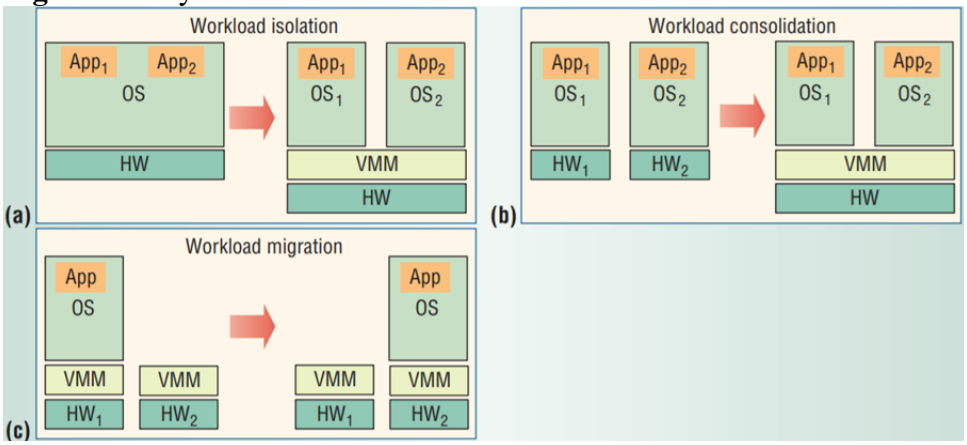
This section introduces the technical concept of virtualization and reducing company costs with this technology. Virtualization software and its functions are introduced, and other security testing tools important for creating a basic model to test the security of an organization using virtualization in a virtual laboratory. Virtual laboratories allow for the emulation of real life cyber threats and the rapid generation of multiple scenarios and infrastructures (Justice & Vyas, 2017).

Virtualization

Virtualization of the physical resources of computing systems to improve and use device sharing has been known for decades. Full virtualization of all system resources including processors, memory, and input/output devices allow one to run multiple operating systems on a single physical platform. In a non-virtualized system, one operating system checks all hardware resources. The virtualized system includes a new layer of software, the virtual machine monitor. The main task of the virtual machine monitor is to decide on the access to the basic resources of the physical hosting platform so it can be used by multiple operating systems which host the virtual machine monitor. The virtual machine monitor provides each guest operating system with a set of virtual platform interfaces that together form a virtual machine (Kryvinska, 2012; Urmila, 2014).

The best-known advantages of virtualization include improved reliability, manageability, and utilization of mainframe systems. Multiple users with different operating systems can easily share a virtualized server. Operating system updates can be performed within virtual machines to minimize maintenance time, and potential failures in the guest software can be isolated to the virtual machine in which they originated (Uhlig et al., 2005; Urmila, 2014).

Figure 2. Ways to Use Virtualization



Note. App = Application; OS = Operating System; HW = Hardware; VMM = Virtual Machine Manager
Source: Uhlig et al., 2005

Workload Isolation

Virtualization can improve overall system security and reliability by isolating multiple software in its own virtual machines. Security is improved by the intrusion or limited intrusion by the virtual machine in which they occur. Reliability is enhanced because software failures in one virtual machine do not affect other virtual machines (Greguš & Kryvinska, 2015; Urmila, 2014).

Workload Consolidation

Increasingly, company data centers face similar problems—a large number of non-monochrome and underutilized servers that run a single operating system and are used by a single application such as web hosting or file delivery. Virtualization enables the merging of individual workstations into a single physical platform, reducing overall operating costs. Another issue is the management of updates. Releasing new hardware or operating systems may create incompatibilities with legacy software, which can limit the entire organization. Virtualization alleviates this problem by allowing both the old and newer operating systems to run simultaneously on a single machine (Urmila, 2014).

Moving Workload Migration

Virtualization allows one to separate guests from the hardware being worked on and move it to another platform. This greatly facilitates hardware maintenance. Moving a virtual machine can be triggered automatically; for example, by balancing the workload (i.e., when individual virtual machines turn on or off according to the workload) or through failure prediction programs, which automatically move the virtual machine to another platform for error detection. These options bring about improved service quality at lower operating costs (Urmila, 2014).

VMware Infrastructure

VMware Infrastructure is a complete suite of virtualization infrastructure for a company. It provides detailed business virtualization, simple management, resource optimization, application accessibility, and operations automation capabilities. VMware Infrastructure virtualizes and aggregates basic physical hardware resources across multiple systems and provides virtual resources to data centers in a virtualized environment. In addition, VMware Infrastructure enables resource allocation, immediate availability, and consolidated backup of the entire virtual data center (VMware, 2019).

Virtualizing and Reducing Company Costs

VMware Infrastructure has been providing a high-level virtualization solution since 1998. A number of studies confirm that virtualization with VMware Infrastructure reduces companies' *Total Cost of Ownership* (TCO) and ensures an almost immediate return on investment. For many technology investments, hardware and software costs are always the easiest to quantify. However, Goldworm and Skamarock (2007) confirmed these costs as only part of the total cost of purchasing technology. The analysis of the total cost of ownership provides a more detailed look at all the factors entering the purchase of new technologies, including the cost of supporting and maintaining the investment over the coming years. Total Cost of Ownership models are a valuable tool for understanding costs and optimizing IT investments. Although the purchase price of a server is the easiest to quantify, industry research suggests that the purchase price usually represents less than 15% of the total cost of ownership (VMware, 2006). Accurate server models should calculate not only the cost of buying, but also the cost of installing, configuring, and managing servers.

Cost Reduction

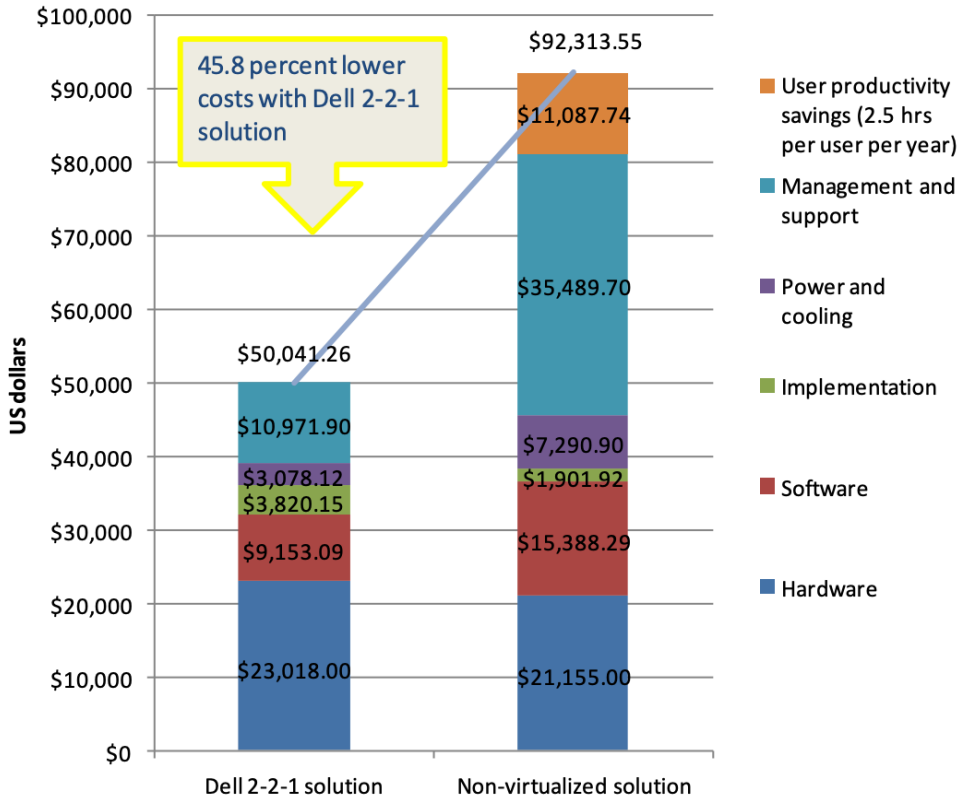
In developing the theoretical basis for this work, we found that by virtualizing the work environment, many companies significantly reduce the total cost of ownership of servers. Therefore, a few numerical examples are presented below. According to Principled Technologies (2011), "one of the most significant benefits of server virtualization is cost savings. The ability to run business

applications on fewer servers reduces the amount of hardware business needs. As a result, the business can gain savings in the following areas:

- fewer servers to buy, service, and manage
- fewer staff hours devoted to server maintenance and management
- lower electricity bills due to less power usage
- less wasted employee productivity due to server downtime
- reduced likelihood of federal and industry regulatory compliance fines due to lost data" (p. 1).

Due to "virtualization, one new physical server can run multiple applications, each on its own virtual machine (VM), while still providing strong performance and offering headroom to spare" (Principled Technologies, 2011, p. 2). Figure 3 is an example comparison of the 3-year TCO of the Dell 2-2-1 solution with the non-virtualized solution. Adding servers to an existing installation for non-virtualized solution is more difficult as it takes up space, is more difficult to manage, and can suffer large amounts of downtime (Principled Technologies, 2011).

Figure 3. Dell 2-2-1 Solution With Virtualization Savings Over a Non-Virtualized Solution in Providing High Availability and Room for Growth



Source: Principled Technologies, 2011

According to Principled Technologies (2011), "a thorough TCO analysis incorporates not only initial costs (i.e., hardware and software purchases), but also includes areas such as power and cooling, implementation and training, and management" (p. 2). The calculated TCO over a 3-year period based on real-world data could save a small or medium business 45.8 percent ($42,272) in costs over a non-virtualized solution (Principled Technologies, 2011). See Table 1 for detailed parameters of the compared devices.

Table 1. Comparison of the Components of the Dell 2-2-1 Solution and the Non-Virtualized Solution

Dell 2-2-1Solution	Non-Virtualized Solution
Decommissioning/repurposing 4 legacy 3-5 year old servers 2Dell PowerEdge™R410 servers, each with 2Intel® Xeon® processor E5630s(2.53Ghz), 24GB of memory, and 2250GB drive sand redundant power supplies	Maintaining 4 legacy 3-5 year old servers 2Dell PowerEdge R410 servers, each with 2Intel Xeon processor E5630s (2.53GHz),16GB of memory, 2250GB drives, and redundant power supplies
2Dell PowerConnect™5524switches	1 Dell PowerConnect 5524 switch
1Dell PowerVault™MD3200istorage array with 12 500GB NL-SAS drives	1 Dell PowerVault MD3200i storage array with 12 500GB NL-SAS drives
Microsoft Windows Server 2008 R2Enterprise Edition with Hyper-V Microsoft System Center Essentials 2010Dell Open Manage Subscription Service	Microsoft Windows Server 2008 R2 Enterprise Edition Dell Open Manage Subscription Service

***Source**:* Principled Technologies, 2011

OpenStack

OpenStack is a free, open-source cloud platform. OpenStack software manages large reserves of storage, computing, and network resources across a data center, managed by a dashboard that gives administrators control while also redistributing resources to users through a web-based interface. The OpenStack cloud platform provides convenient solutions, especially for organizations managing and operating large IT infrastructures. It provides an open and flexible system for creating a software-defined infrastructure. OpenStack supports the development of the agility and agility management of its own application portfolio and enables companies to provide automated, self-service, and secure services (Blokdyk, 2020a).

The OpenStack platform is integrated with all major Linux distributions, hypervisors (virtual machine monitors) and software-defined storage. In addition, it provides access to and use of other open-source technologies. OpenStack can be integrated to some extent with existing virtualized infrastructures based on VMware (Blokdyk, 2020a; Silverman & Solberg, 2018). There are many variants of model development of OpenStack with various functionalities and options. See Figure 4 for a model of the OpenStack deployment with best practices for high networking security. To isolate sensitive data communication between the OpenStack networking services and other OpenStack core services, communication channels should be configured to only allow communication over an isolated management network (OpenStack, 2021).

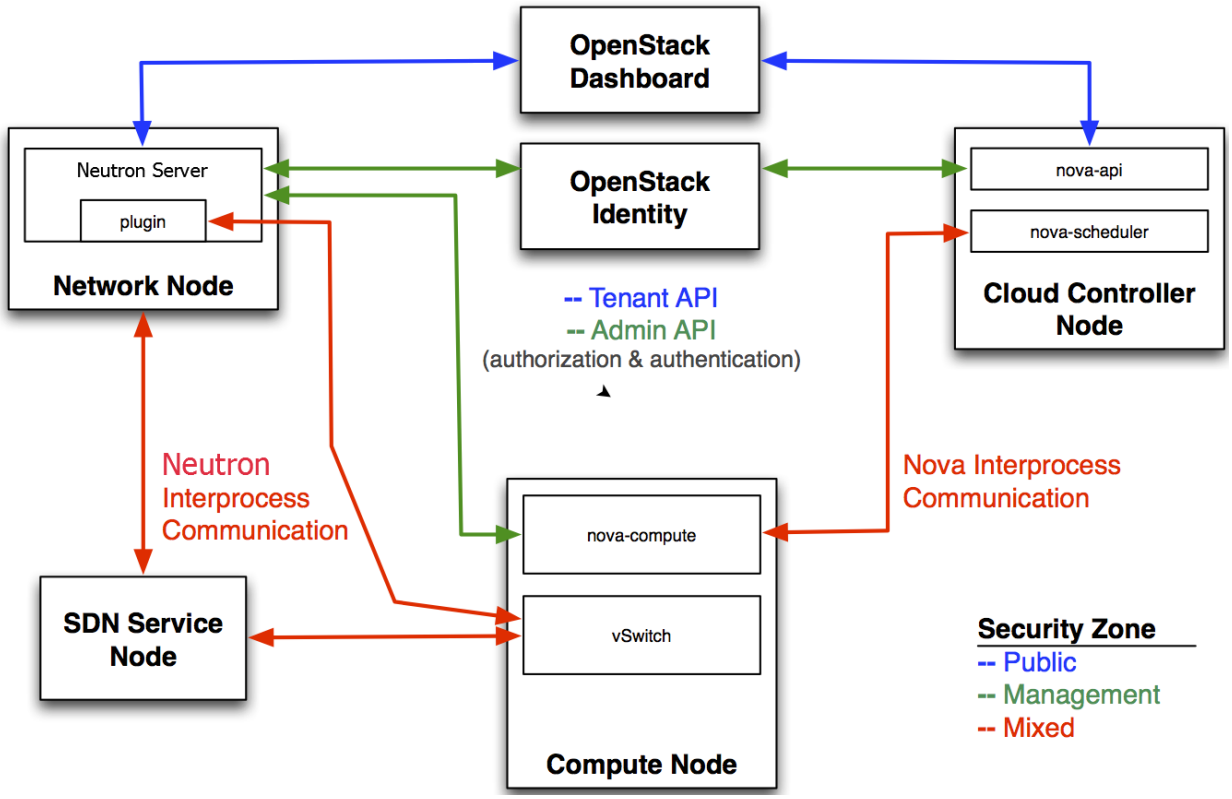
Kali Linux

Although the term Linux is commonly used as the name for the entire operating system, Linux is merely the name of the kernel—the software that handles hardware-end user interactions. The term Linux distribution refers to a complete operating system that is built on the Linux kernel and usually includes an installer and a number of pre-installed or ready-to-install applications. Debian GNU/Linux is a leading Linux distribution known for its stability and quality. Kali Linux builds on the work of the Debian project and adds more than 300 of its own special application security packages, especially in the field of penetration testing. Debian is a free software project that provides multiple versions of the operating system (Velu & Beggs, 2019).

Kali Linux is one of the most powerful and most used security testing tools worldwide. Frequently used by security experts, it provides a wide range of applications, from penetration testing, forensic analysis, and reverse engineering to vulnerability assessment. Kali Linux is the result of continuous development of the platform, from WHoppiX (the Linux distribution for penetration testing, later

renamed WHAX), to BackTrack (the direct predecessor of Kali Linux). Today it is a comprehensive penetration testing system that draws on many features from the Debian GNU/Linux distribution and with the support of the global open-source community. Kali Linux was not designed as a simple toolkit, but rather as a flexible system providing user-level customization. Professional testers, security enthusiasts, students, and amateurs can thus adapt functions to their specific needs (Hertzog & O'Gorman, 2017).

Figure 4. OpenStack Deployment With High Networking Security



Source: OpenStack, 2021

Methods

Work Methodology and Examination Methods

This section describes the methodology used in the production of this work. In this work, we examined the practical use of virtualization in a business environment. The objective was carried out using the OpenStack platform, in which the model of the work environment was built, and its vulnerability tested. The resulting recommendations were prepared based on a theoretical background and on tests of the security of the virtual work environment.

The methodology of the project was based on an analysis of the available literature on technical advice, the literature in the field of management and economics, and an analysis and preparation of internet resources. The empirical part of the work was realized by creating a model of the environment for security testing purposes. This work used methods of analysis, deduction, comparison, and synthesis.

Characteristics of the Examination Object

The research object was the work department of a public limited company where the authors work. The main tasks of the work team are preparing financial analyses, payroll analyses, and reports and creating presentations for the management. The department creates and controls invoices and performs accounting and administrative activities. Department members work with all types of data and use spreadsheet software for their work. The physical environment where the work team operates was moved to the virtual environment.

Working Procedures

The workflows consisted of analyzing and processing the theoretical background, analyzing the entire enterprise, analyzing the work team, designing an optimal model for workspace virtualization, creating a virtual workspace model using the OpenStack platform, testing the security of the model, and drawing conclusions and recommendations. The acquisition of the input data for the empirical part was carried out by observing the work environment in the organization at a specific point in time. The output data were obtained and interpreted based on experience.

Data Collection and Resources

While processing the research and collecting information for the theoretical part, the information was mainly drawn from foreign sources. Specifically, electronic and Internet resources, relevant online documents, official program documents or statements, newspaper articles, presentations, secondary data in the form of financial analyses or scientific studies, and technical literature in the fields of management, business, and informatics were used. Company data was obtained by observing the working environment, and the benefits of virtualization were evaluated based on the results of the experiment.

Methods of Evaluation and Interpretation of Results Used

The evaluation of the obtained empirical data was carried out based on the outputs of the experiment—testing the security of the virtual work environment. The results were interpreted using methods of analysis, experiment, comparison, and synthesis.

Technological Background of the Experiment Model

The basis of the experiment was created in the OpenStack environment on the Stein version. OpenStack was installed and configured as a clean installation specifically for the purpose of experimenting on a single server as a single node solution. Infrastructure network modeling was based on a best practice model for high networking security (see Figure 4). The solution was fully managed as a software defined network. It was based on OpenStack Neutron server technology which was needed for complex network management and modeling. For high performance, whole computation Was done by OpenStack Nova server with Kernel-based Virtual Machine (KVM) hypervisor and hardware acceleration. For the experiment, the server HP ProLiant DL580 Gen7 with 24 physical cores, 196 GB of RAM, and 300GB hard drive space was used. Base on the operating system running OpenStack services, Linux CentOS version 7 was used.

Description of the Company

The company has been operating in the global market for decades, offering a range of IT services ranging from cloud-based solutions to data analysis, statistics, resource, and facility management to industrial solutions such as banking or telecommunications. It has several branches in Slovakia and employs several hundred employees.

The hierarchy of management is divided as follows. The employees work in teams and each team is dedicated to its own classification. Outputs from one team can then be used by another team in their work. Each team has one manager through which all requests pass (such as requests for access to databases, requests for new workstations, etc.). Applications always go through several levels of authorization until they are approved or rejected. The team manager is also responsible for maintaining work ethics and good team relationships, solving complaints and non-compliance with work procedures, promoting learning and development, and keeping track of team members' attendance.

The building is divided into several floors and each floor has its own floor manager, superior to all team managers. The floor manager is usually the highest ranking manager in a branch and ensures the smooth running of the branch, solves problems of the team managers, mediates information from other branches, prepares work plans, and checks the team managers' observations of their teams. Above the floor manager are several levels of management (middle and top level) whom the authors, however, do not meet during work.

Every employee has their own laptop computer, to which they can request a monitor, mouse and keyboard, holder, and so on. Communication in the company takes place by e-mail via intranet or by phone or video calls. Upon onboarding, each employee is assigned an account which logs into the in-house network and for which they request the necessary access to perform their work activities. With this account, they log into the intranet network, from which they have access to databases, mail, online storage, and the like. At the same time, the movement of the employee on the network is monitored for security reasons.

Each personal computer is encrypted, secured with multiple layers of passwords, and secured with a Kensington security slot. Employees must enter their username and password each time they sign in. A back-up program is always running in the background that regularly backs up data on hard drive to the cloud. Access to many websites is restricted for security reasons. Every computer constantly displays its location and is checked several times a day by an antivirus program. All applications required for work are available from the intranet, so no disk installation is required. At the entrance to the building, it is necessary to show the access card as well as at the entrance to the individual floors. Security officers check the floors several times a day, otherwise they are available at the main entrance of the building at the front desk.

The company operates on several continents, from America to Europe to Asia. Servers that connect to employees are adapted to this—if they are in Europe, they connect to servers in Europe. Server rooms are spread across several countries, especially in the United Kingdom. Therefore, the authors do not have detailed information to ensure this.

Findings

This section presents the results of the practical part of the project. An environment model was created to test its security. The company where the modeling was performed and the authors' experience with the company are described. The model is presented whereby the physical environment of the company was transferred to a virtual one. The security of information systems was tested based on this model. The discussion evaluates the outputs of the practical component of the project and combined with new knowledge acquired during the processing of the theoretical part of the article. Finally, recommendations are made to streamline work in the company.

Internal Background of the Company

During the recruitment process, each employee is made aware of company policy and the obligations with which they must comply. Of all the obligations, special mentions should be made of the confidentiality agreement and the duty to protect business secrets. After accepting the job, the employee is provided with a work computer, which must be completely set up from the beginning. To do this, the employees use the instructions supplied with the computer. After installing the operating system and initial login, employees must select a pin code used to unlock it. Subsequently, the employee logs into the company's intranet network using the assigned credentials, allowing them to finalize the system installation. Using provided links, the employee then clicks through to a page that allows them to install the programs needed to perform their work.

No authors were checked during or after the installation of the operating system. Although the installation instructions were written quite clearly, it was obvious that it had not been updated for a long time. For example, the instructions referred to the installation of programs that were not currently available. We also referred to the installation of a modern version of the programs, but later in found that we needed an older version for data compatibility. The instructions did not contain any reference to certain precautions such as the hard disk encryption obligation, which was only announced to the authors after some time spent in the company. The authors encountered no other problems.

The mood was relaxed in the workplace. Relations between employees are good, often reinforced by team building, various group tours, social events, or workshops. Communication between management and employees is mostly via email, when all employees are simultaneously informed about current events in the company. Employee education takes many forms. The authors most often encounter online courses, which usually take two to three hours to complete, and are completed with a test that requires at least 80 percent correct answers to pass.

The main drawbacks the authors encountered during their work in the company were system failures and long authorization times. System failures are rare (3-4 times a year), but they significantly delay work, as teams tend to be interdependent. An authorization period is connected with waiting for permission to access databases, where the authors had to wait three months to grant access to a specific database needed to perform their work.

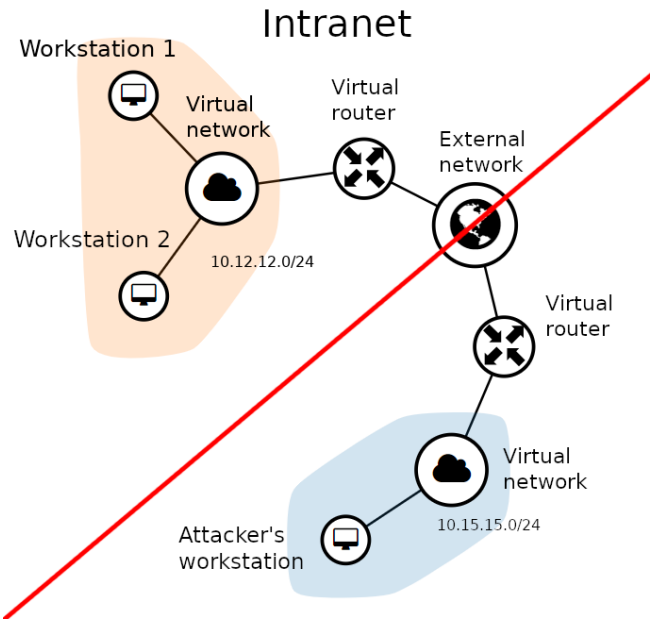
Model

The work team where the authors are assigned was chosen as a template for virtualizing the work environment and creating a security testing model. The work team has the task of preparing financial analysis, payroll analysis, and reports and creating presentations for management and controlling

invoices, accounting, and administrative work. The work team works with data of all kinds and very often uses spreadsheet-supporting software.

In terms of time savings and the overall complexity of virtualization for most companies, it was concluded that a simple model was sufficient for these work purposes. The virtualization model of the work environment and the testing itself were implemented in the OpenStack platform. Figure 5 shows the virtual workspace model.

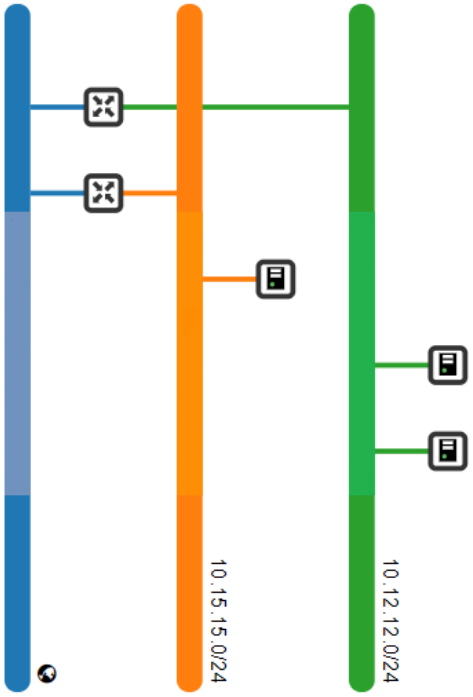
Figure 5. Virtual Workspace Model



The model in Figure 5 shows a work team connected to the local, in-house intranet connected to an external network. There are two workstations in the orange area (Workstation1, Workstaton2) illustrated by a monitor icon and connected to the company's intranet with the network address 10.12.12.0/24, represented by a cloud icon. The four arrows represent a router that connects workstations to an external network, and the globe represents the external network—the Internet. In the blue area is an attacker's workstation that attempts to attack the work team and test the security of the virtual environment. The attacker's workstation is connected to a private network with a network address of 10.15.15.0/24, and this network is connected to an external network through a router. The red line represents the imaginary separation of the network and the environment between the company and the attacker.

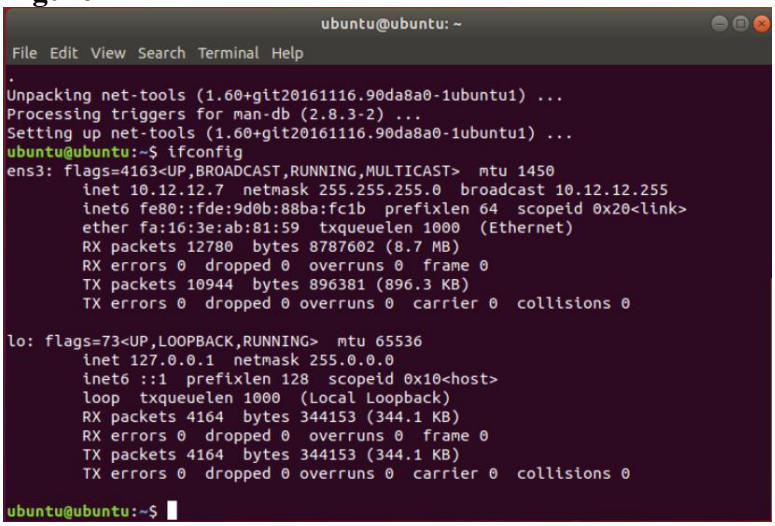
Another view of the model is the network topology (see Figure 6), which displays how each workstation and network device is connected to each other. The picture was generated directly from the OpenStack dashboard. The green area represents the working environment in the company to be tested—two workstations connected to the local in-house network. The orange area represents the attacker's local network, its workstation, and its connection to an external network. The blue area represents the external network—the Internet.

Figure 6. Network Topology



Employee workstations migrated to the virtual environment in the form of the Ubuntu Linux distribution. Ubuntu distribution provides employees with the same capabilities they currently have in a physical environment, making it easier to install and run quickly. To save time, an immediately executable version of the software was used without the need for installation. The distribution was kept in the basic version, and no extra software was installed. With virtualization, it was possible to run several workstations without problems, but in the end two were enough for testing (see Figure 7).

Figure 7. Ubuntu Linux Workstation



Using the ifconfig command specified in the Ubuntu distribution command line determines the workstation's IP address. This matches the address displayed in the network topology (10.12.12.7 for the first workstation and 10.12.12.5 for the second workstation). If necessary, work can be started immediately in this virtual workstation. The attacker's workstation was migrated to the virtual

environment in the form of the Kali Linux distribution. The distribution pre-installed more than 300 applications for penetration testing and security audit. The ifconfig command specified in the Kali Linux distribution command line could also be used to determine the IP address of a workstation that matches the address displayed in the topology (10.15.15.3).

The ping command tested the connection speed between a Kali Linux instance and two Ubuntu workstations. The ping command sends a packet to the destination computer, which responds to it and evaluates how long the response is received, or simply lists whether there is a connection. In this case, three and four packets were sent to both stations with a response time of 2037 and 3004 milliseconds.

Each instance had a public or floating address in addition to its own, private, fixed IP address. While private IP addresses were used to communicate between instances, public IP addresses were used to communicate with networks outside the cloud platform (such as the Internet). Currently, two floating IP addresses are used out of a total of fifty floating IP addresses.

Security groups are a set of rules for filtering IP addresses out of all project instances, deciding on network access. By default, a security group prevents any incoming data traffic and only allows traffic that originates from a particular instance. It is assigned one security group to the instances out of a total of ten security groups. From block storage, twenty gigabytes of the total number of thousands of gigabytes are used. Instances were assigned one volume per block.

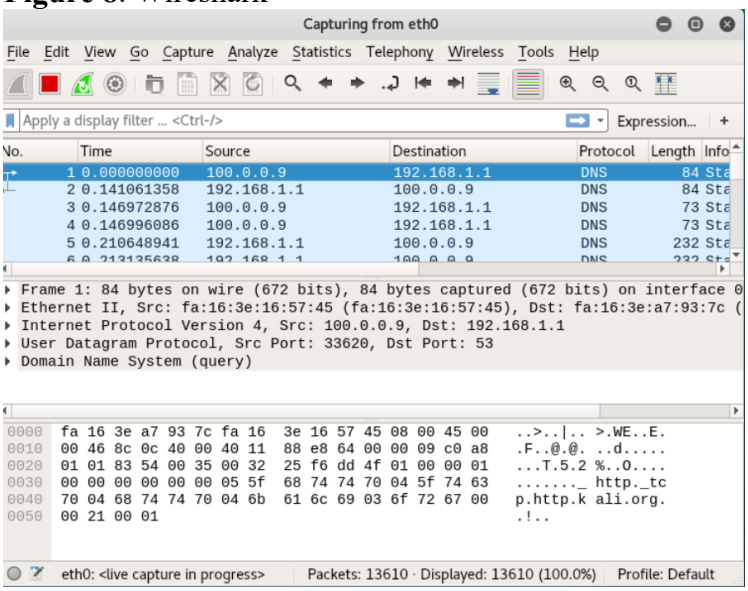
Security Testing

To avoid disseminating instructions for a specific infiltration of the company, the work does not include specific security test procedures. The security tests were performed using the Kali Linux distribution and the OpenStack platform. There were a number of infiltration testing tools to choose from, including network infrastructure testing, packet capture, port, and IP address verification using Wireshark, Nmap, and Sparta.

Wireshark workstation is constantly receiving or sending data through. Wireshark collects all this data and displays it for later use. Monitoring the data transfer from the workstations was able to detect the IP addresses of individual instances, track their movement on the network, and even capture the data transfer when it tried to send a password over an unsecured Hypertext Transfer Protocol (HTTP) protocol. It was also capable of intercepting voice transmissions over the Internet Protocol, isolating the transmission of packets over IP, and listening in on a short conversation between two employees. However, most other transmissions were encrypted using the Secure Shell (SSH) protocol used to transmit data over unsecured networks (the Internet), and the captured data could not be traced back to its original content (Hack, 2019). Figure 8 shows Wireshark in the context of the Kali Linux virtual instance.

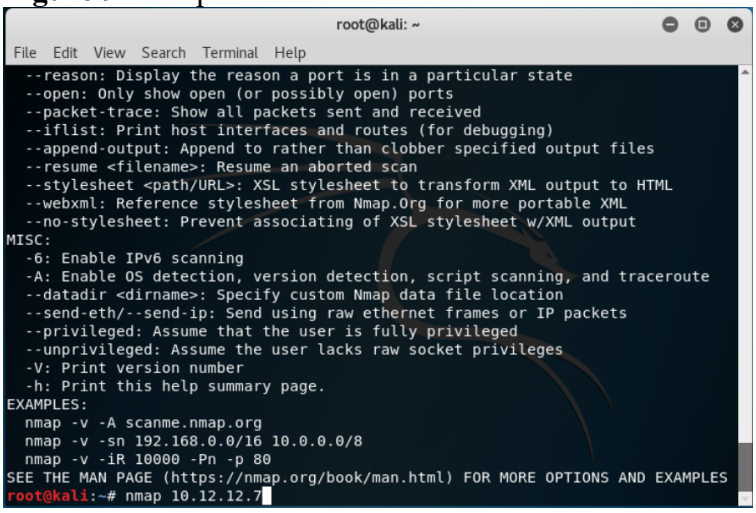
The Nmap, or Network Mapper, is a tool used to map and explore a network (Sharma, 2019). Using the Nmap command associated with the destination IP addresses (10.12.12.5 and 10.12.12.7), which were detected in a previous test and examined in more detail, a network scan was initiated. The scan result revealed several shortcomings. It was possible to find out what versions of operating systems the workstations are using (Ubuntu), and it was also possible to detect used packet filters.

Figure 8. Wireshark



The Nmap command scans a thousand ports by default and then prints results showing whether the ports are open, closed, or filtered. When a port is open, it usually waits to receive protocols such as Transmission Control Protocol (TCP), Stream Transmission Control Protocol (SCTP), or User Datagram Protocol (UDP). An open port is a common target for attackers, so administrators try to close or secure it with a firewall. A closed port does not receive any cues, but since it can be opened at any time, an attacker can keep it backed up and scan it again at a later time; so, it is worth considering securing closed ports with a firewall. The filtered port is secured by a firewall or other way of blocking access to the port, so Nmap cannot determine whether it is open or closed. Port testing revealed that some had been opened, which posed a significant security risk. Figure 9 shows Nmap against the background of a virtual Kali Linux instance.

Figure 9. Nmap

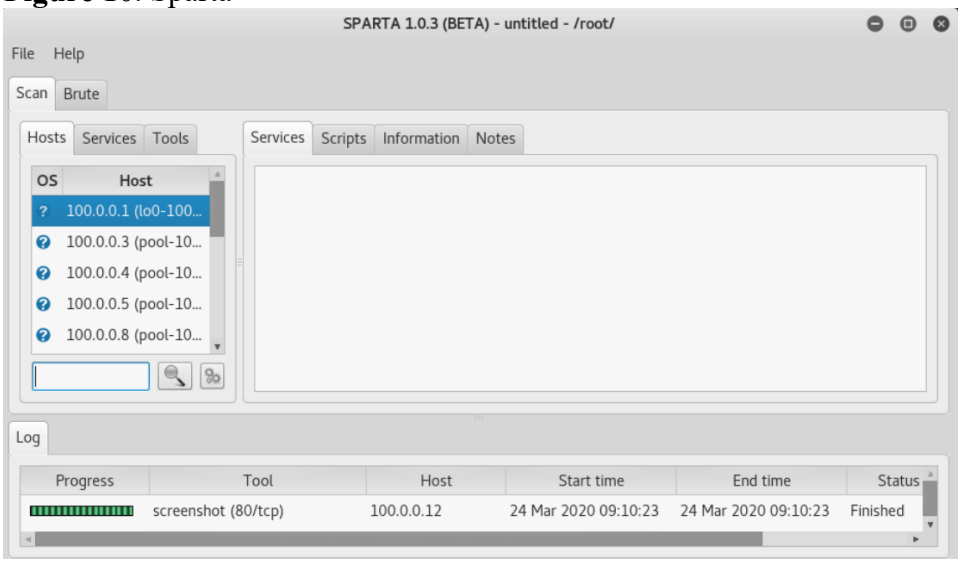


The Sparta results from previous Nmap testing were also used in the Sparta testing. Nmap outputs were saved as an extensible markup language (XML) file and uploaded to Sparta, which saved time considerably as other services could be tested in more detail on the prepared port list. Sparta allows assignment of an automated list of tasks to each identified service, such as scanning HTTP protocols

or testing Secure Sockets Layer (SSL) protocols. This helps, for example, identify system vulnerabilities, misconfigured web servers, or detection of ciphers used for network communications. The tool is also capable of a so-called *brute force attack*, which attempts to decipher encryption without prior knowledge of the encryption key. It is a continuous testing of combinations of a certain set of login data and passwords. However, the time required to decipher the key increases exponentially with its length.

Testing with Sparta can scan a list of workstations and servers on the network. Sparta does visualization of services visible on the network. The use of the brute force attack is possible after scanning services are listed. If there is service protected by a password or users account credentials, it can be attacked with word lists of passwords, or detected login data such as username and password for FTP. Figure 10 shows Sparta in the background of a virtual instance of Kali Linux captured in the scanning processes.

Figure 10. Sparta



The Results of Security Tests

This part of the article describes the modeling result for penetration testing. For modeling, a solution based on OpenStack technology was built. For a specific solution, a small data center was built for the penetration testing. In a specific test example, three virtual machines based on Linux technology were used. Furthermore, two neutron routers and two software defined networks were used. Specifically, the virtual machines included various services such as samba, ftp, sftp, various types of Web Distributed Authoring and Versioning (WebDAV) servers, or web other application services. We did not extend the scope of the test in our paper. The aim was to make a model of the infrastructure for network tests and mapping purposes. From the point of view of the security test, a port scan was performed on the whole subnet range. The result of the test was the discovery of two done and two Ubuntu desktop virtual machines on the network. For these virtual machines, no application components could potentially create security risks or security holes. However, the model was built on the real network architecture. This model is used very often in combination with the client server in practice. To simplify the model, only desktops without application bases were used to model the architecture. Modeling the specific architecture could be expanded quickly by specific modules or servers on which it is possible to perform testing in a few quick steps without having to interfere with

the real infrastructure. The conclusion of the test was the output of successful modeling of the environment for the purpose of safety testing.

Conclusions

The objective of this work was to create a model for security testing in an organization through virtualization (see Figure 5 for the virtual workspace model). The model was created based on a specific work team from an unnamed company. It was not possible to create a model of the entire company due to time and overall demands. The model was created using the OpenStack platform, which allowed the authors to migrate the entire work team infrastructure from the physical environment to the virtual environment.

At the end of the experiment, a functional virtual workspace was available and offered employees the same capabilities as the physical environment. This allowed employees to continue working in a virtual environment in the event of a system failure. Similarly, the security manager was able to test the security of the information systems in a virtual environment without restricting the operation of the company through forced shutdowns. With the help of simple penetration tests, the security of the virtual environment could be tested. Testing the security of the company environment through virtualization was successfully carried out. The company has since developed a guide on how to virtualize part of the work environment.

Theoretical Implications

The present work offers contributions to theory. The model made is applicable to other work teams with a similar infrastructure. As a result, the company may consider introducing virtualization in other departments. Regarding information security, the tightening of data protection laws (GDPRs) has led many organizations to focus intensively on the security of information systems, mainly due to liquidation fines of up to twenty million Euros or 4% of the company's annual turnover. By virtualizing the work environment, we managed to streamline the process of information security solutions in the company. We have shown that penetration testing in a virtual environment is possible and necessary. The security information environment in the company then brings additional benefits. If an organization meets international information systems security standards (such as ISO 27 001), it automatically becomes more trustworthy and can attract new business partners. In terms of legislation, the Act on Cyber Security applies to the Slovak Republic, laying down minimum requirements for the security of public administration information systems and providers of basic and digital services. One of the main objectives of the law is to create a standardized framework for cyber security. Virtualization in this area facilitates the solution and testing of information systems security, thus helping the organization to comply with applicable laws.

In terms of increasing resource efficiency, as shown in the cost reduction comparisons of organizations, organizations often use only a small amount of available hardware resources. In terms of cost savings, reducing the number of servers also reduces the costs associated with deployment, operation, maintenance, security, and support. All the companies mentioned in the comparison that opted for virtualization have experienced a multiple return on investment as early as six months after virtualization was introduced. At the same time, total hardware and software cost of ownership has been reduced by approximately 70%.

In terms of saving time and maximizing productivity, by testing security in a virtual environment, system downtime was minimized, and subsequent testing was performed without affecting the productivity of employees and the whole organization. The testing was performed without any interference of the real infrastructure.

From the point of view of self-evaluation of the organization because every day the methods of industrial attacks and data theft increase, it is important for organizations to make security testing a permanent, repetitive process. This is possible due to a virtual work environment that does not affect the physical environment. It provides security staff with an ideal space to improve the current situation and test new trends in information security. With subsequent evaluation of the security of information systems, the organization can take preventive steps for the future.

Practical Implications

Based on the results of the empirical part of this project and the processing of information in the theoretical part of the article, the following practical recommendations were prepared for organizations. It is recommended to virtualize part of the work environment or the entire work department based on the model in this work. The model should be modified to the specific needs of the organization. We would like to emphasize a more efficient use of hardware resources and the ability to test security regardless of the physical environment, to minimize planned outages, and to perform the tests without affecting the normal operation of the organization.

It is recommended that companies consider virtualizing either a group of servers or entire server rooms. Because system failures were often observed during quarterly outages, which caused significant complications and delays, this step would significantly reduce server load during critical periods. At the same time, it would reduce the total cost of owning servers, increase the use of hardware resources, and reduce the time required to resolve planned and unplanned outages. Companies are encouraged to ensure strict compliance with information and cyber security laws to increase control over the recruitment and training of new employees to prevent possible future data leaks.

Limitations and Future Research

The main limitation of the work is the demanding migration of complex hardware interfaces. Due to the overall complexity of virtualization for the entire organization, we decided to virtualize it. During the elaboration of the theoretical part of the work, new facts emerged that were used in the empirical part of the work and in formulating conclusions and recommendations.

The formulation of the final findings and recommendations was based on the theoretical background as well as the outputs of the empirical part of the work. The virtual work environment provided several advantages over the physical environment. It has enabled information security to be addressed independently of the physical environment, minimizing downtime, and maximizing company productivity. Hardware resource utilization maximized potential cost savings by reducing the number of servers when deciding to virtualize most of the company. It facilitated compliance with applicable laws, regulations, and standards. It also allowed the organization to acquire a picture of the current state of information security. Future research should focus on more comprehensive modeling of the architecture of technological solutions and processes in the organization.

References

Allen, M. (2019). *The chief security officer's handbook: Leading your team into the future*. Academic.

Blokdyk, G. (2020a). *OpenStack solutions a complete guide*. 5STARCooks.

Blokdyk, G. (2020b). *Information systems security engineering a complete guide*. 5STARCooks.

Brodin, M. (2019). A framework for GDPR compliance for small- and medium-sized enterprises. *European Journal for Security Research, 4*(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

Calder, A., & Watkins, S. G. (2019). Information security risk management for ISO 27001 / ISO 27002 (3rd ed.). ITGP.

Černá, M., & Sieber, R. (2018). Approach of selected business entities to GDPR implementation. *ACC Journal, 24*(2), 20-31. https://doi.org/10.15240/tul/004/2018-2-002

Diogenes, Y., & Ozkaya, E. (2019). Cybersecurity – Attack and defense strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals (2nd ed.). Packt.

European Commission. (2018). *The GDPR: New opportunities, new obligations: What every business needs to know about the EU's General Data Protection Regulation*. Publications Office of the European Union. https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf

European Commission. (2019). *Digital government factsheet: Slovakia*. European Commission https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovakia_2019.pdf

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer.

Goldworm, B., & Skamarock, A. (2007). *Blade servers and virtualization: Transforming enterprise computing while cutting costs*. Wiley.

Greguš, M., & Kryvinska, N. (2015). *Service orientation of enterprises—Aspects, dimensions, technologies*. Comenius University in Bratislava.

Hack, P. J. (2019). *Hacking Linux: The complete beginners programming system guide with practical hacking tools and essentials basics of hack–Includes Kali Linux step by step, security testing and penetration testing*. Independently published.

Hertzog, R., & O'Gorman, J. (2017). *Kali Linux revealed: Mastering the penetration testing distribution*. Offsec.

Hobart, M. E., & Schiffman, Z. S. (2000). *Information ages: Literacy, numeracy, and the computer revolution*. Johns Hopkins University.

Hoofnagle, C. J., Sloot, B. V. D., & Borgesius, F. Z. (2019). The European union general data protection regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2–18. https://doi.org/10.1108/OIR-11-2015-0358

Intersoft Consulting. (n.d.). *GDPR: Fines / penalties*. Retrieved January 9, 2020, from https://gdpr-info.eu/issues/fines-penalties/

International Organization for Standardization. (2018). *Information technology—Security techniques—Information security management systems—Overview and vocabulary*. (ISO Standard No. 27000:2018). https://www.iso.org/standard/73906.html

Justice, C., & Vyas, R. (2017, June 25). *Cybersecurity education: RunLabs rapidly create virtualized labs based on a simple configuration file* [Conference presentation]. ASEE Annual Conference and Exposition, Columbus, OH, United States.

Kaczor, S., & Kryvinska, N. (2013). It is all about services-fundamentals, drivers, and business models. *Journal of Service Science Research, 5*(2), 125–154. https://doi.org/10.1007/s12927-013-0004-y

Karande, P., Gaherwar, S., & Kurhekar, M. (2015, August 13). *Physical to virtual migration of Ubuntu system on OpenStack cloud* [Conference presentation]. Third International Symposium on Women in Computing and Informatics, Kochi, India.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security, 25*(3), 300–329. https://doi.org/10.1108/ICS-02-2016-0013

Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

Kryvinska, N. (2012). Building consistent formal specification for the service enterprise agility foundation. *Journal of Service Science Research, 4*(2), 235–269. https://doi.org/10.1007/s12927-012-0010-5

Marget, A. (2021). *Downtime: Causes, costs and how to minimize it*. Unitrends. https://www.unitrends.com/blog/downtime-causes-costs-and-how-to-minimize-it

Molnár, E., Molnár, R., Kryvinska, N., & Greguš, M. (2014). Web intelligence in practice. *Journal of Service Science Research, 6*(1), 149–172. https://doi.org/10.1007/s12927-014-0006-4

Ofori, K. S., Anyigba, H., Ampong, G. O. A., Omoregie, O. K., Nyamadi, M., & Fianu, E. (2020). Factors influencing information security policy compliance behavior. In. W. Yaoukumah, M. Rajarajan, J. Abdulai, I. Wiafe, & F. A. Katsriku (Eds). *Modern theories and practices for cyber ethics and security compliance* (pp. 152-171). IGI Global.

OpenStack. (2021). *Networking services security best practices*. OpenStack. https://docs.openstack.org/security-guide/networking/securing-services.html

Oracle. (n.d.). Introduction to Oracle® Solaris 11.2 virtualization environments: Virtualization technology models. Retrieved April 8, 2021, from https://docs.oracle.com/cd/E36784_01/html/E36847/virttechnologies.html

Principled Technologies. (2011). *TCO benefits of server virtualization for the small and medium business*. Principled Technologies. https://www.principledtechnologies.com/clients/reports/Dell/2-2-1_virtualization_TCO_1111.pdf

Sebetci, O. (2020). An investigation of the effects of information system literacy and business process management on organizational performance. *Journal of Global Business Insights, 5*(2), 87–102. https://doi.org/10.5038/2640-6489.5.2.1134

Sharma, H. (2019). *Kali Linux – An ethical hacker's cookbook: Practical recipes that combine strategies, attacks, and tools for advanced penetration testing* (2nd ed.). Packt.

Silverman, B., & Solberg, M. (2018). *OpenStack for architects: Design production-ready private cloud infrastructure* (2nd ed.). Packt.

Uhlig, R., Neiger, G., Rodgers, D., Santoni, A. L., Martins, F. C. M., Anderson, A. V., Bennett, S. M., Kagi, A., Leung, F. H., & Smith, L. (2005). *Intel virtualization technology. Computer, 38*(5), 48–56. https://doi.org/10.1109/MC.2005.163

Urmila, R. P. (2014). Cloud computing with open source tool: OpenStack. *American Journal of Engineering Research, 3*(9), 233–240.

Velu, V. K., & Beggs, R. (2019). *Mastering Kali Linux for advanced penetration testing: Secure your network with Kali Linux 2019* (3rd ed.). Packt.

VMware. (2006). *VMware infrastructure architecture overview*. VMware. https://www.vmware.com/pdf/vi_architecture_wp.pdf

VMware. (2019). *VMware TCO comparison calculator*. VMware. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmware-tco-comparison-calculator-methodology-whitepaper.pdf

Wahl, T. (2020). *Commission evaluation report on GDPR*. Eucrim. https://eucrim.eu/news/commission-evaluation-report-gdpr/

Zetoony, D. (2019). *The EU GDPR General data protection regulation: Answers to the most frequently asked questions*. American Bar Association.