

Virtualization safety

Zh E Aytkhozhaeva, A A Ziro, A Zh Zhaibergenova*

Kazakh National Research Technical University, associated professor, Satpayev Str. 22, Almaty, Kazakhstan

**Corresponding author's e-mail: zhanshuak@gmail.com*

Received 13 March 2017, www.cmnt.lv

Abstract

Article considered virtualization technologies, their types, advantages and disadvantages. Attention to specific risks and information security threats in case of virtualization platforms is paid. The main risks of virtualization platforms are defined. Potential internal vulnerabilities of virtualization platforms can be revealed only by testing for penetration which user-friendly and available instrument for implementation is specialized by Kali Linux OS. The attacks to the virtual machines with use of the Kali Linux tools were organized. As a result of experiments is Kali Linux allows revealing and analyzing vulnerabilities at the channel, network and transport levels. For detection of problems at the level of applications that is urgent for virtualization of platforms, it is necessary to use commercial products of ethic hacking in addition.

Keywords:

virtualization platforms,
risks,
penetration testing

1 Introduction

Virtualization technologies, along with cloud computing, take key positions among the advanced and perspective trends in IT area since 2009 (according to the analytical company Gartner). Taking into account that virtualization technologies are the fundament of cloud computing, it is possible to give with confidence a prize-winning place of virtualization without which cloud computing are unrealizable. Much of advantages and disadvantages of virtualization technologies automatically reflected in cloud computing.

Virtualization technologies passed the already considerable way of the development from purely scientific interest and decisions for insulation of computing environments of different tasks within one mainframe before creation of the virtual area networks and program containers encapsulating a complete set of the virtual hardware resources [1].

In a general view there is the type of virtualization: virtualization of resources. Virtualization technologies resources historically gained earlier development and recognition- the multiprocessor systems, clustering of computers, grid computing, the virtual area networks, etc. Virtualization technologies platforms began to develop later. Now actively develop and progress, have a set of different types of implementation are cornerstones of cloud computing.

Deployment on one physical server of a set of the virtual servers which ensure functioning of any operating system gives big advantages and absolutely new opportunities [2]. Prospects of technology of virtualization of platforms are also defined by it. But wide recognition and application restrains existence enough serious shortcomings of this technology [3].

Experience shows that many projects on virtualization were comprehended by failure. Nearly a half of the companies (44%) which made virtualization attempts can't claim about their successful completion. This is due to the difficulty of assessment of resetting of investments, and to

complexity and high cost of deployment and support of corporate virtual infrastructure.

2 Virtualization disadvantages

Appearance of new poorly studied and low-probed risks and security risks of information when using virtualization including in cloud computing also belongs to shortcomings of technology. This weakness is compounded by the fact that different types of virtualization of platforms bear specific risks and threats due to specifics of the implementation.

Physical, logical and program structures are a defining factor for appearance of risks and threats of information. In architecture of the computing systems used in the virtual decisions nothing changed. Therefore the basic conventional principles of support of information security shall be observed also in such systems. Virtualization not to a lesser extent needs protection and a judgment on its bigger safety thanks to the most structure doesn't respond the reality. On the contrary, specific risks and security risks of information in case of virtualization of platforms in addition take place, as well as in case of any new technology. The main problem constraining development and implementation of virtualization of platforms is the problem of protection of such systems. Use of standard checked methods and security features in case of virtualization platforms, in that look in what they exist now isn't enough. In case of virtualization of platforms of property of a physical medium exist in the form of program settings. And it is simpler to change program settings illegally.

For example, the standard security reference monitor (a resident component of safety) controlling loading processes can't perform the functions when loading the virtual machines. At the same time the resident component of safety shall be present and have access to the controlled environment. For the virtual environment there shall be specific mechanisms of monitoring. By operation in the virtual environments of

virtualization platforms the situation changes very quickly. New components are quickly created and together with them also new potential threats are created. At the time of creation of the virtual machine it isn't protected in any way. Constant control of a situation is necessary.

The solution is complicated by the fact that architecture of systems of virtualization different for different types of virtualization platforms. For example, depending on a type of virtualization platforms, the hypervisor, being the manager (monitor) of the virtual machines (compact highly specialized OS), is set or on "bare iron", or/and on OS. There are also such types of virtualization (virtualization at the level of an operating system) when the hypervisor isn't used.

The expression that virtualization ensures the best information security, is based only that on the virtual machines it is simpler to set rules of a network access. The statement, that vulnerability of a hypervisor and probability of the attack to it very low, is based that there is no information on the attacks to hypervisors. It isn't confirmation of either absence of the attacks, or high safety of hypervisors.

There is no accuracy of an exception of risks and threats of virtualization of platforms exist. Besides, now virtualization technologies begin to be applied to violation of confidentiality, integrity and accessibility of information more and more actively. The research Blue Pill project which visually showed how technologies of the hardware virtualization can be applied in the espionage purposes (the Blue Pill program including a hypervisor) is known. Now Blue Pill is a code class name of root kits (the programs hiding presence at system of malicious software) based on use of the hardware virtualization.

3 Risks and threats of virtualization

The research of risks and information security threats when using virtualization is an urgent problem, both in respect of safety of the virtual infrastructures, and in the theoretical and practical development plan and advances of technologies of virtualization.

It is necessary to define the main risks of virtualization platforms:

1. a uniform point of a failure in a failure mode of the physical server;
2. a uniform point of a failure in a hypervisor failure mode (in case of its existence) and/or hosts OS (in case of its existence);
3. risk of a compromise of a hypervisor of the virtual machines (in case of its existence) and/or hosts OS (in case of its existence);
4. implementation of a hypervisor in the form of software module is more vulnerable to the attacks, than hardware or software implementation;
5. risk of a compromise of data by memory transmission (local storage) from one virtual machine to another;
6. violation of insulation of processes (virtual machines), basic principle of virtualization;
7. risk of a nonadjustable data migration of limited access;
8. a possibility of network attacks between the virtual machines (virtual servers) located on one physical server;

9. the known decisions on program virtualization aren't provided with protection at the hardware level on TPM technology (the specification describing the trustable module which makes available to an operating system guaranteed safe services). Even in new technologies of the hardware virtualization a part of the mechanism of virtualization is implemented by the software of a hypervisor.

There is a nonzero probability of existence of the hidden or functional vulnerabilities of a hypervisor and possibility of carrying out the attack against it:

1. the risks connected to increase in mobility and use of the virtual machines in architecture of cloud computing;
2. the unrolled virtual systems often don't conform to requirements of a corporate policy of information security.

Operations in the field of minimization of new risks and threats of virtualization technologies of platforms are carried in different directions. Some of them are provided below.

Good hypervisors contain the virtual switchboards and firewalls which settle down between physical interfaces of the server and the virtual interfaces of the virtual machines. Protection against network attacks between the virtual machines (virtual servers) located on one physical server is provided (in the absence of a compromise of a hypervisor of the virtual machines).

For the hypervisors Microsoft, IBM, Citrix and VMware companies gives a guarantee of insulation of processes and data of the virtual machines from each other. It is considered that it provides a possibility of safe information processing of different level of privacy on single physical device.

The Symantec Company offers the Symantec NetBackup™ platform with V-Ray technology which on the basis of patent decisions provides evident representation of the virtual machines and applications on physical and virtual servers. The technology of backup and restoration for the environments VMware and Microsoft Hyper-V, quickly selective recovery of data from the applications working under control of hypervisors of VMware and Hyper-V is implemented.

The AMD company developed AMD-V technology in which a special protect mode of start of the monitor (hypervisor) of the virtual machines is realized. The Intel Company used the previous TPM 1.2 specification (the last TPM 2.0 specification) for increase in security in one of the chipsets (technology of safety LaGrande/TXT).

Even this short list of operations shows, risks of virtualization of platforms are how various. At the enterprise using technologies of virtualization it is necessary to clarify - what risks threaten business processes at present and to estimate these risks [4]. In case of estimation of risks assessment of probabilities of events as the risk is a combination of probability of an event and its consequences are executed.

$$R = S * E, \quad (1)$$

where R is the risk, S is the extent of damage, E means probability of an event.

For detection of potential internal vulnerabilities and assessment of probability of an unauthorized event, including in case of virtualization platforms, it is possible to use penetration tests. During testing the tester (auditor)

models actions of the malefactor, trying to break information security of a subject to protection. Search of vulnerabilities of system of protection and their subsequent use is executed. Now testing for penetration is one of the information security systems recognized around the world as method in case of the active audit. There is a standard on conducting testing for penetration [5]. There are different programs for conduct testing for penetration (ethic hacking), including specialized Kali Linux OS [6]. The Kali Linux tools allow executing search of operation of vulnerabilities in Web servers, wireless protocols, communication links, mobile devices, applications. Having set Kali Linux on single virtual machine, it is possible to attack other virtual machines, as for the purpose of testing for penetration, and unauthorized obtaining information.

4 Detection of vulnerabilities by means of testing

In an experiment the virtual machines created in VMware Workstation were used. Having set Kali Linux on one virtual machine, the attacks to other virtual machines for the

purpose of testing for penetration and unauthorized obtaining information were organized. Results of some of them are given below.

One of the methods of detection of vulnerabilities is port scanning of the virtual machines by means of the network Wireshark analyzer. Wireshark analyzer is the application of the Kali Linux. Wireshark analyzes the traffic passing through the network interface of the computer that allows viewing completely contents of the transferred packets at all levels. Wireshark listens to all network traffic and captures it.

In a Figure 1 the results received by Wireshark by the analysis of the traffic passing on wires through ports of one of the virtual machines are provided. In a Figure 1 the flow of network packets which can be analyzed is visible. It is visible that the system of virtualization VMware is used. Contents of the packet both sent, and received can be opened, having executed click on it. We obtain information on port and the IP address of the sender, port and the IP address of assignment, the transfer protocol, lifetime of a packet, etc.

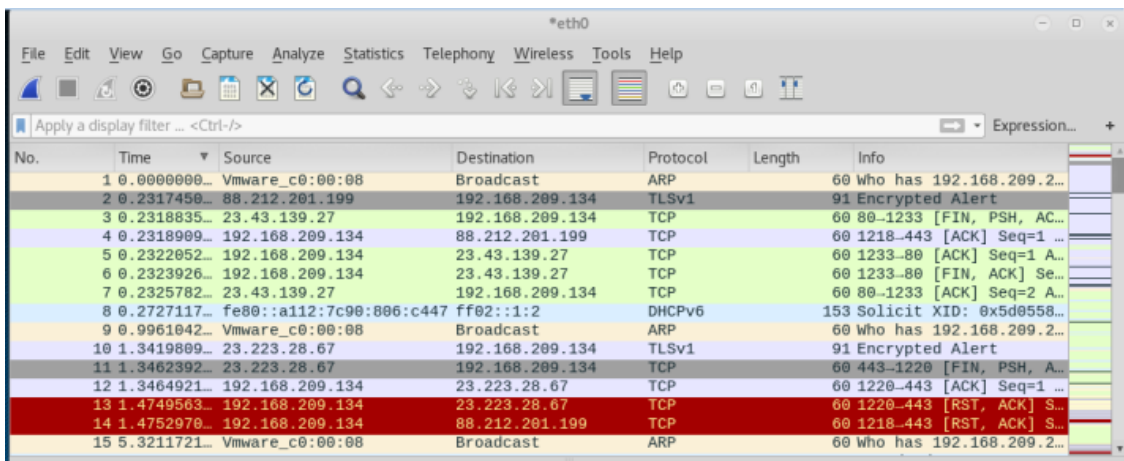


FIGURE 1 An example of the scanned traffic

Packets can be filtered in a set of parameters. It is possible to set the filter for receiving the traffic meeting certain requirements. By means of the "http.request.method == "POST"" filter it is possible to intercept login and the password, to obtain information on a frame, the version the protocol Internet, the data transfer protocol, the hypertext transfer protocol. In a Figure 2 in the upper part the selected

packet from the intercepted flow of packets which contents reveal below is shown. It is visible that the packet of HTTP is encapsulated in a packet of TCP (transport layer), the packet of TCP is encapsulated in IP (network layer), and IP is in turn encapsulated in Ethernet. In the lower part of a Figure 2 the HEX code is shown.

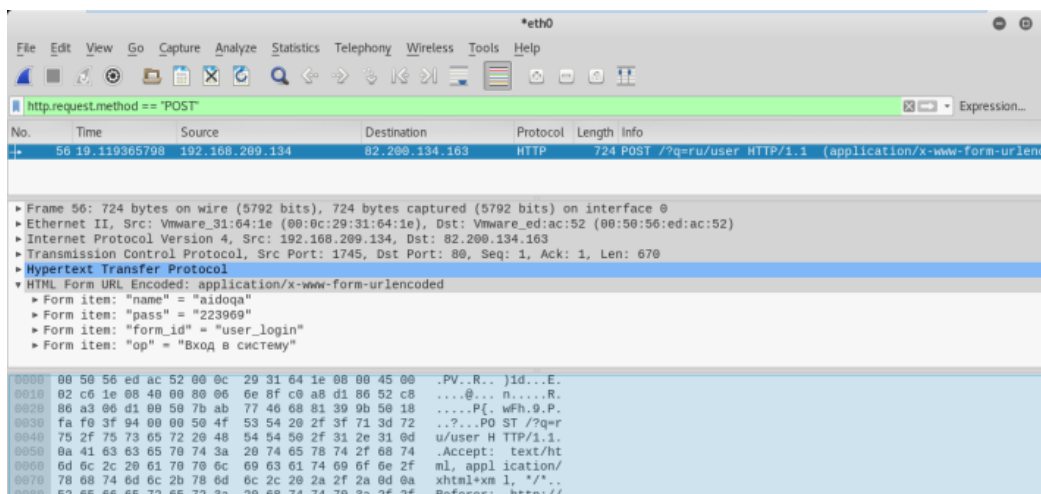


FIGURE 2 An example. Interception of data

Disclosing the level of each protocol, we obtain the detailed information from each level. In a Figure 2 information of a packet 56 of HTML forms is shown. The login and the password entered by the user are defined. If to open the most top line, it is possible to obtain general

information about a frame.

Information on a packet of 2572 from the Ethernet level is shown in a Figure 3. Information about destination, source address and type of IP (IPV4) is presented.

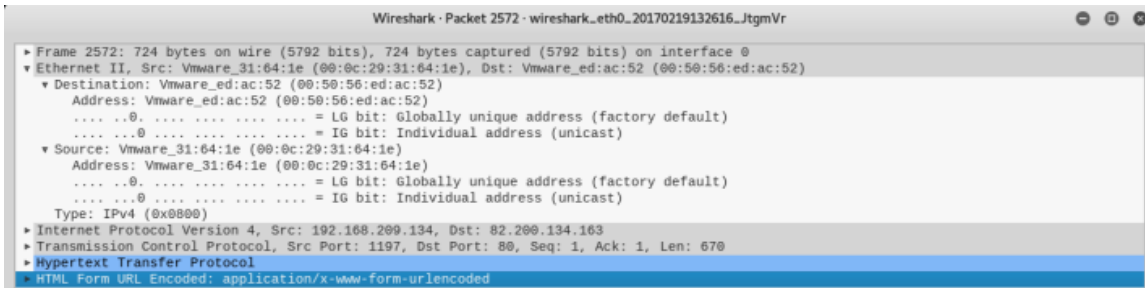


FIGURE 3 An example of the intercepted data (from the Ethernet level)

In a Figure 4 is shown information on a packet 2572 about differentiated services, flags, destination GeoIP. from the IP (IPV4) level. The figure includes information

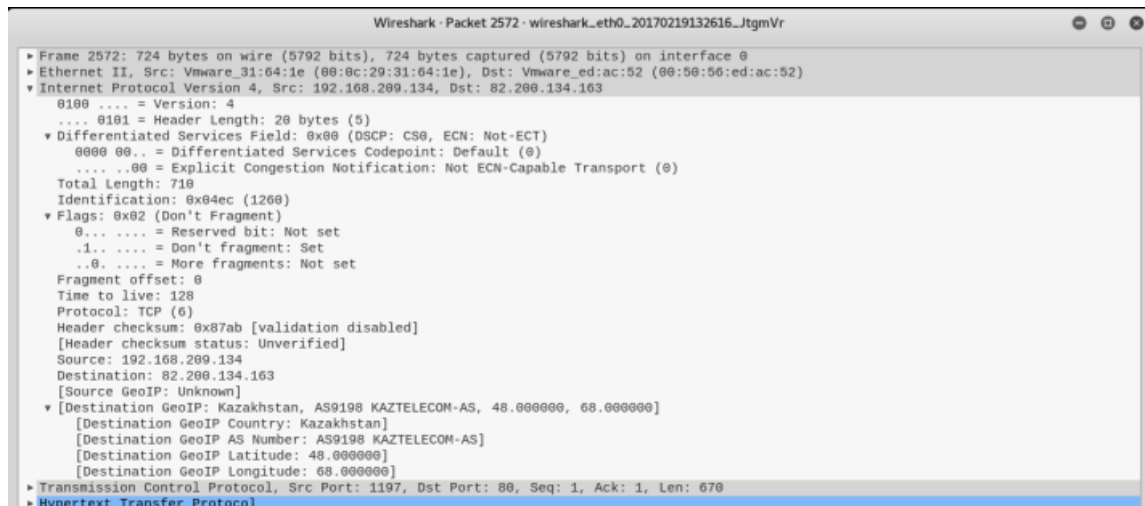


FIGURE 4 An example of the intercepted data (from the IP level)

Information on a packet of 2572 from the TCP level is shown in a Figure 5. Figure defined source port, destination port, flags and etc.

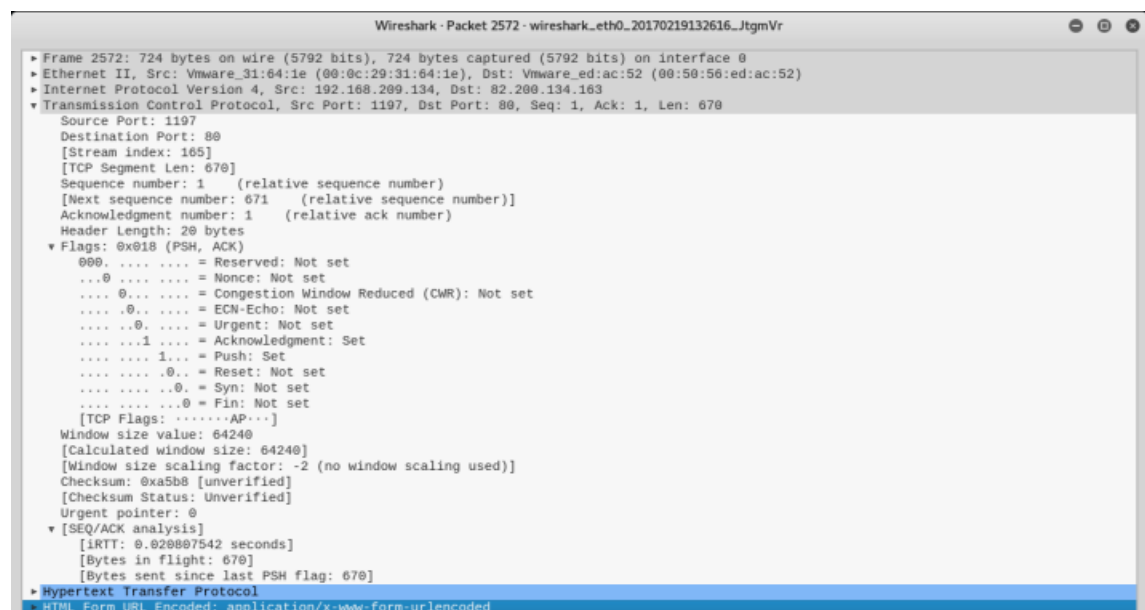


FIGURE 5 An example of the intercepted data (from the TCP level)

Information on a packet of 2572 from the HTTP level is shown in a Figure 6. Information about request method, host, content-length and cookie is presented.

In case of use of cryptography protocols (in this case TLS), a part of the intercepted information will be ciphered

and the level of the ciphered sockets will be visible (Figure 7). Figure defined TLSv1, handshake protocol.

In case of interception of the ciphered data they can be decrypted by using the appropriate settings.

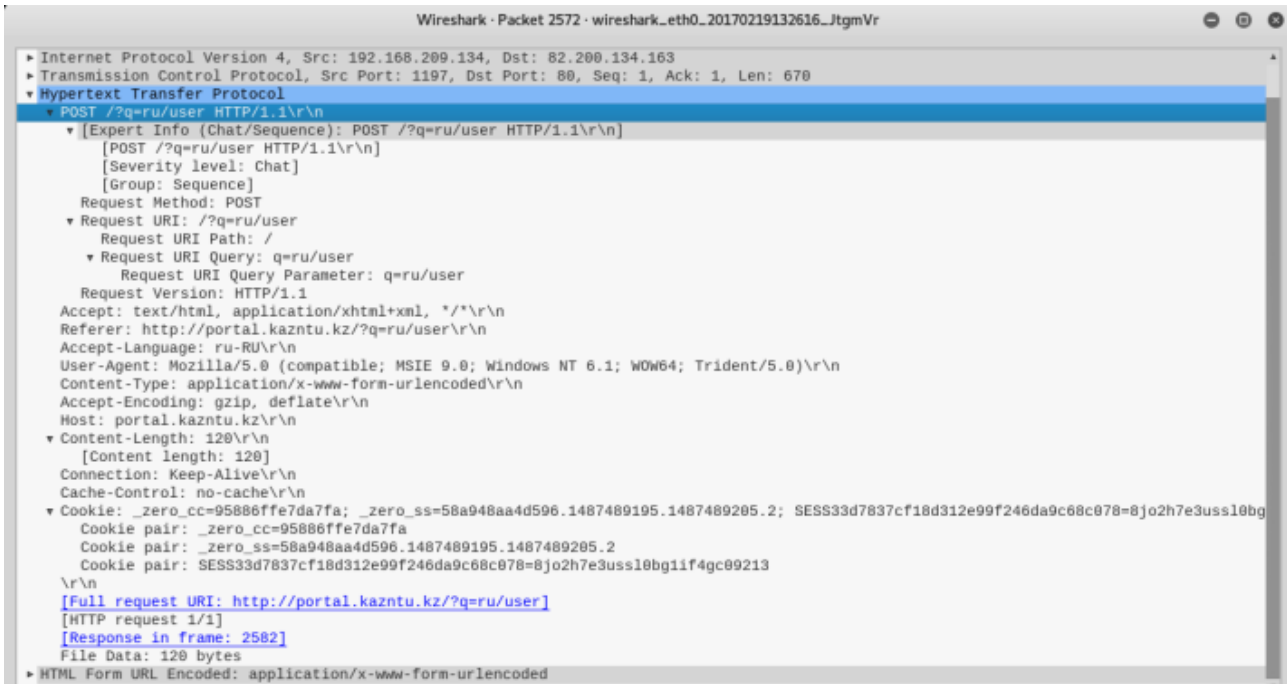


FIGURE 6 An example of the intercepted data (from the HTTP level)

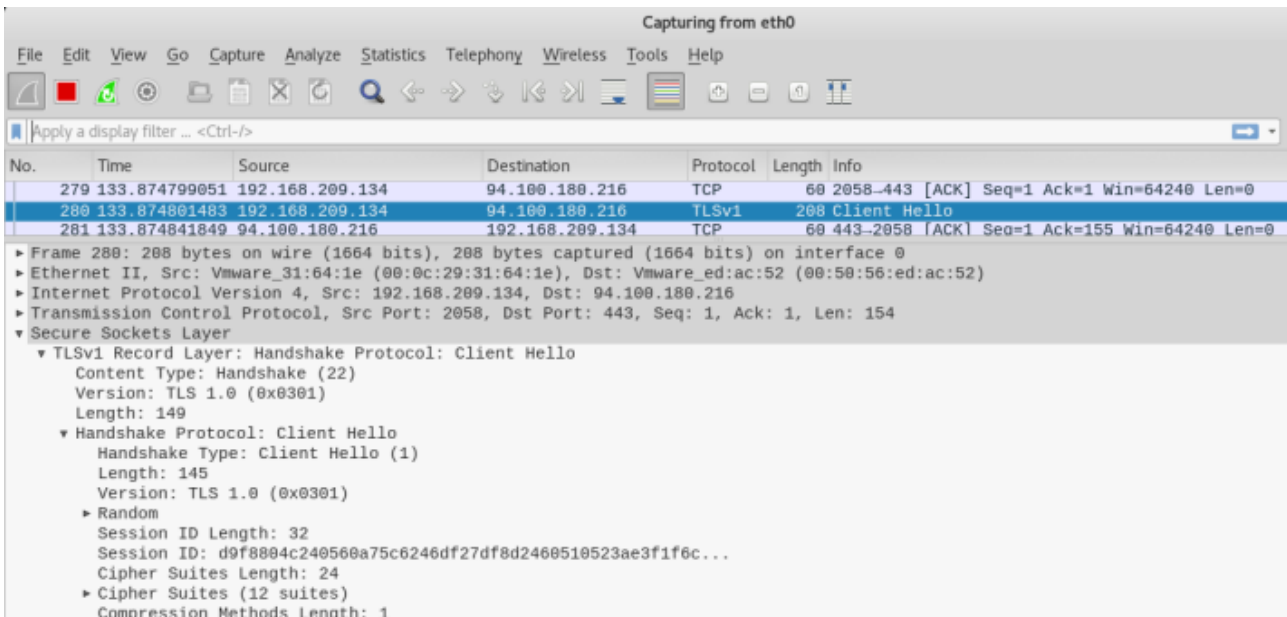


FIGURE 7 An example. Interception of the ciphered data

5 Conclusions

Virtualization is not only perspective strategic technology which has specific risks and threats. The vulnerabilities of platform virtualization need to be identified considered and minimized, including by means penetration testing. Free products of penetration testing are easy to use. They allow identifying vulnerabilities on the channel, network and transport levels, having built-in expert systems. When




solving problems at the application level, these products unusable. In this case necessary to use commercial solutions. Commercial products of the penetration testing use more advanced technologies and have extended capabilities compared to free ones. This provides additional opportunities in assessing risks and threats. Platform virtualization works on the application level. Therefore, penetration testing should be performed on both the channel, network and transport layers, and at the application level.

It should be remembered that virtualization platform technologies can be applied also in illegal purposes to violation of information security. Virtualization gives new

opportunities, but also place of IT professionals more demands, both in respect of professional level, and in respect of level of responsibility and ethics.

References

- [1] Portnoy M 2016 *Virtualization Essentials* John Wiley & Sons: Indianapolis p. 309
- [2] *The Advantages and Disadvantages of Virtualization* Milner 2015 <http://milner.com/company/blog/technology/2015/07/14/the-advantages-and-disadvantages-of-virtualization/> 15 Feb 2017
- [3] Ziro A A, Aytkhozhaeva E Zh 2017 Trend virtualizatscii i ego osobennosti III *Mezhdunarodnaya nauchno-practicheskaya konferentsiya: Fundamental'nye Nauchnye Issledovaniya: Teoreticheskie i Practicheskie Aspekty ZapSibNTS: Kemerovo pp 206-9 (in Russian)*
- [4] ISO/IEC 27005:2011 Information technology Security techniques Information security risk management *International Organization for Standardization* 2011 http://www.iso.org/iso/catalogue_detail?csnumber=56742/ 1 Feb 2017
- [5] Information Supplement: Penetration Testing Guidance *PCI Security Standards Council* 2015 https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf 1 Mar 2017
- [6] Official Kali Linux Documentation *Kali* 2014 <https://www.docs.kali.org/kali-linux-documentation/> 9 Mar 2017

Authors	
	<p>Evgeniya Aytkhozhaeva, 1947/02/01, Republic of Kazakhstan</p> <p>Current position, grades: associated professor of the Department of Information Security, Candidate of Technical Sciences University studies: St. Petersburg State Electrotechnical Institute (Technical University "LETI"), Russia Scientific interest: Information Security, Databases Systems, Hardware of Cryptography Publications (number or main): over 160 Experience: more than 30 years of scientific and pedagogical experience</p>
	<p>Aasso Ziro, 1992/01/01, Republic of Kazakhstan</p> <p>Current position, grades: tutor of the Department of Information Security University studies: ITMO University, Russia Scientific interest: Information Security Publications (number or main): 7 Experience: 1 year</p>
	<p>Zhanshuak Zhaibergenova, 1993/06/17, Republic of Kazakhstan</p> <p>Current position, grades: tutor of the Department of Information Security University studies: ITMO University, Russia Scientific interest: Information Security Publications (number or main): 6 Experience: 1 year</p>