Письма в ЭЧАЯ. 2016. Т. 13, № 5(203). С. 1000–1005

VIRTUALIZATION IN EDUCATION: INFORMATION SECURITY LAB IN YOUR HANDS

A. A. Karlov [1]

Joint Institute for Nuclear Research, Dubna

The growing demand for qualified specialists in advanced information technologies poses serious challenges to the education and training of young personnel for science, industry, and social problems. Virtualization as a way to isolate the user from the physical characteristics of computing resources (processors, servers, operating systems, networks, applications, etc.) has, in particular, an enormous influence in the field of education, increasing its efficiency, reducing the cost, making it more widely and readily available. The study of Information Security of computer systems is considered as an example of use of virtualization in education.

PACS: 01.30.Cc; 01.50.H-; 01.50.Qb; 07.05.Bx

INTRODUCTION

Over the recent years the activity of cyber criminals increased significantly in all areas: theft of money from credit cards and racket, industrial espionage and sabotage, attacks on the state organizations, etc.

Stock markets are a new front in cybercrime: a powerful insider data theft scheme was discovered in the USA. It allowed getting hundred million dollars by trading on the sensitive internal corporative information [1].

Hacking the website of the US Tax Service brought criminals about $50 million, while more than 100 thousand personal records of people were stolen in 2014 [2].

Stuxnet was a very sophisticated cyber attack against the Iranian nuclear programme. The SCADA (Supervisory Control and Data Acquisition) software from Siemens was infected and a full control over PLCs (Programmable Logic Controllers), responsible for the rotational speed of the uranium enrichment centrifuges, was obtained. Variation of the rotational speed of centrifuges over the month put them out of action and made useless [3].

Cyber attack on metallurgical plant in Germany caused significant damage. Attackers were able not only to get access to the plant control system, but put it out of operation. First, hackers took control of the e-mail of the factory workers by sending them letters with phishing links. Through e-mail of employees, hackers gained access to the enterprise network and then to the entire control system of the plant [4].

[1] E-mail: Alexander.Karlov@cern.ch

Stealing personal data of millions of the Americans in the cyberattacks on the US Office of Personnel Management (OPM) allowed to compromise the data on special operations and employees of several intelligence agencies, including the CIA and the NSA [5].

Confidential data of 1,500 US military personnel (e-mail addresses, passwords in an unencrypted form, places of work, phone numbers, etc.) were stolen [6]. There are many other examples.

It is clear that only highly qualified specialists in the field of information security can constrain an impact coming from cyber criminals' threats. But today, in the US only, more than 200,000 information security jobs are unfilled [7]. Globally, by 2019 there will be 6 million information security professionals needed [8]. Thus, the training of specialists in information security becomes a critical task on a national scale.

Virtualization of information systems has an important role in the effective training of specialists in information security due to significant advances in hardware and software virtualization technologies. It allows changing the paradigm in the approach to education. Instead of lectures in the classroom and students doing "homework", a professor can give students the fundamentals and then students have to do practical work in a classroom. At the same time, the constant self-study should take place for both students and professionals to learn and use the latest advances in information technology. This is especially true for information security specialists.

THE OLD DAYS

By itself, virtualization is not a new approach. In the late 1960s and early 1970s, IBM was thinking about how to allow several users to use one system and run several applications (time-sharing). That was when the first hypervisor appeared on System/360 (CP-40 and then CP-67). The early hypervisor gave each mainframe user the so-called conversational monitor system (CMS), essentially a single-user operating system. The hypervisor provided the resources while the CMS supported the time-sharing capabilities. CP-67 enabled memory sharing across virtual machines (VMs) while giving each user his own virtual memory space. The hardware-assisted virtualization came later on the System/370 with VM/370, the first virtual-machine operating system. Practical learning how to use a mainframe required a mainframe itself and was very expensive.

While there was a clear need for virtualization on the mainframe in the 1960s, the idea of building hypervisors for new platforms was abandoned during the 1980s and 1990s, when client–server applications and inexpensive x86 servers and desktops led to distributed computing. In the 1980s and early 1990s, x86 servers lacked the horsepower to run multiple operating systems, and they were so inexpensive that enterprises would deploy dedicated hardware for each application without a second thought. But over time, the performance of microchips has increased so dramatically that the typical Windows machine needs less than 10% of the processing power actually delivered by a server today.

BIRTH OF MODERN VIRTUALIZATION AND FURTHER ADVANCES IN IT

It is not until the end of the 1990s when a small Silicon Valley company with less than 20 employees tried to bring virtualization to x86 family of processors. Their first product VMware Workstation was delivered in May 1999. At the beginning, the task for VMware was difficult, because x86 processors had no support for virtualization at that time and the overhead for the CPU was very high. Later, in 2005–2006 Intel and AMD released their limited hardware virtualization extensions to x86 architecture called VT-x and AMD-V.

Since then, the virtualization of information systems has begun. Software and hardware were not the only technologies evolving rapidly. Networking and Internet also developed rapidly and hugely impacted education in Information Technology. Particularly, this gave rise to the phenomenon called MOOCs — Massive Open Online Courses — the Internet gateway to education in a form of free courses available around the world (http://moocs.com/).

Certainly, the IT industry becomes more and more complex, students must learn faster and faster, and professional education plays a more important role. The IT teaching and learning 10 years ago were very different from what they are now. Today all students have personal portable computers. No computer classes (in the early 2000s sense) remain. Thanks to technology advances students and professionals can learn from where they want at the pace they want. Everybody is also much more flexible with respect to practical exercises, since basically it is possible to deploy various types of environments using virtualization on a portable computer.

INFORMATION SECURITY

Information Security was developing hand in hand with other domains of Information Technology. It deals with protecting information confidentiality, integrity and availability and generally tries to decrease the probability that something bad could happen to the information.

Obviously, to protect something against bad things one has to know what they are. Sun Tzu, a Chinese military general, strategist, and philosopher (544–496 BC) wrote: “It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.”

The problem of today’s digital society is that people are not aware of information security risks. Assessment of risk depends on two main variables: the probability of the event and consequences of the event:

$$\text{risk} = \text{probability (threat exploits a vulnerability)} \times \text{impact}.$$

The *impact* of external criminal interference can be pretty well estimated from the technical, economical and political points of view in the business or activities of public and state organizations. But it is much more difficult to estimate the *probability* of a criminal intervention that can exploit vulnerabilities of software and hardware of computer systems. This requires, first of all, the presence of specialists able to search, investigate, and manage various possible attacks on the given information system in its virtual representation.

This means that a specialist in information security, first of all, should have practical experience in dealing with unauthorized access to computer systems. Computer security is fundamentally a practitioner’s art and it demands continuous practice.

Thus, training of students in the field of information security should be based mainly on intensive practical work after getting the basic concepts and fundamentals in lectures. The future professionals have to be able themselves to improve their knowledge adequately to meet the challenges of the time. That is where today’s technology is coming to the rescue: one can simulate an entire company’s network, a datacenter, a website, or a mail server on his own portable computer.

TYPICAL PRACTICAL TRAINING

Integrated practical training of students may consist of the following stages. First of all, the students have to study solutions of practical tasks at the laboratory under supervision of a professor. A typical setup for laboratory practice would consist of the attacker machines (students) and the target services, servers or network (professor's notebook) (see the Figure).

With modern computing power of a notebook a professor can deploy several VMs on his portable computer. A modern notebook can have a processor with four cores, each of which is independently capable of performing two threads (e.g., Intel Core i7-4710HQ quad-core processor), 16 MB RAM and 1TB internal HDD. In other words, a professor can install several virtual machines on his notebook. The installed VMs may contain the same or different vulnerabilities depending of a teaching plan. Modern virtualization products, such as VMware, allow creating fairly complex network topologies including web servers, mail servers, firewall, switches, etc. To avoid help from outside, a professor can arrange an isolated class network and assign to each student his own task to be solved.

Students' knowledge acquired during the laboratory work can be checked in the following way:

— Practical tasks (VMs with vulnerabilities of different types) are prepared by the professor and deployed to the University computing facilities. Professor can use a wide range of virtualization tools and software to arrange various configurations of VMs, servers, network elements, etc., which include vulnerabilities of different types.

— There is a fixed period of time when the solutions of the tasks have to be sent by students back to the professor.

— A professor evaluates the results of students and conducts a joint analysis of the solutions and the difficulties encountered.

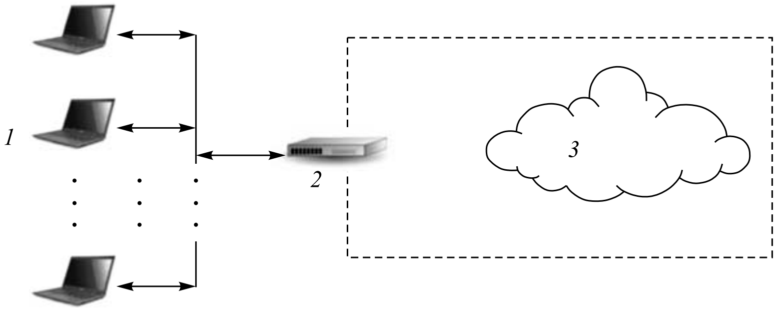
The next step is when each student has to prepare his own example (the own challenge) of VM (website, database, etc.) with one or more vulnerabilities and describe how these vulnerabilities can be used for unauthorized access. As a rule, a professor prepares the list of vulnerabilities' category, for instance:

— Web (hacking web-sites, web-applications, or web-users);

— Crypto (breaking client-side encryption);

— CrackMe (reverse engineering);

— Exploitable (to get control/ownership);



Virtualized laboratory: *1* — students' notebooks (attackers); *2* — virtual or real switch; *3* — virtualized environment (applications, services, infrastructure)

— Forensics (collection and examination of digital media to detect or prevent unauthorized intrusion), etc.

The student has to prepare a complete and detailed report of his challenge and its solution with all files/VM necessary to deploy and test his proposal.

SELF-TRAINING

There are a lot of web sources for self-training which can be and have to be used to extend and keep the professional skill up to date. All these sources are based on the virtualized approach to learning. Internet sources and tools to be used depend on the goal.

— To start with information security, one can download a VM called Metasplitable and deploy it on VM environment of his notebook. Metasploitable is a Linux distribution built for testing security tools and learning penetration testing. How to install and use Metasploitable can be found on www.offensive-security.com/metasploit-unleashed/requirements/.

— Kali Linux (www.kali.org) is another possibility to start learning by creating attacking machine with many necessary security tools.

— A whole virtual vulnerable network can be installed with NETinVM, that is a VMware virtual machine image containing a series of Linux machine capable to run as a virtual network. NETinVM helps a lot in understanding HTTP connection, a capture and analysis of network data traffic, etc. More details are on http://informatica.uv.es/_carlos/docencia/netinvm/netinvm.html.

— From Vulnhub site (www.vulnhub.com) one can download vulnerable VMs that are created by other users and try to attack and exploit them by searching for vulnerabilities. As is mentioned on the site, the Vulnhub goal is "to provide materials that allow anyone to gain practical 'hands-on' experience in digital security, computer application and network administration".

Thanks to virtualization, many websites are proposing online security challenges to teach web security, reverse engineering, cryptography, and system hardening. Some examples can be found on www.root-me.org, www.hackthissite.org, www.w3challs.com, www.try2hack.nl.

Capture the Flag competitions (CTFs) are also powerful training in the field of information security in the form of digital battles where multiple teams compete against each other. Concerning computer security competitions, CTFs are arranged in the way to give an experience both in the search for vulnerabilities and attack the opponent's VM, on the one hand, and to protect its own VM or small VMs network from external attacks, on the other hand.

To be successful, the participants have to use a wide range of tools for network sniffing, penetration testing, system administration, protocol and traffic analysis, etc. A limited time (for example, 48 h) and the emulative spirit stimulates them to strengthen and expand the knowledge in information technology, to understand better the behavior of criminals in organizing of attacks. The participation in CTFs is a great way to learn and keep the information security skill up-to-date.

Thus, virtualization as a way to isolate the user from the physical characteristics of computing resources (processors, servers, operating systems, networks, applications, etc.) has an enormous influence in the field of education, increasing its efficiency, reducing the cost, making it more widely and readily available. Education, especially in the field of information security, is a continuous process that begins with students' studies and that must constantly accompany a professional activity of information security specialist. Today, it's high time to do so.

REFERENCES

1. *Anand P.* Traders Busted after Enlisting Hackers to Play Stock Market to Net $100 Million // MarketWatch. Aug. 11, 2015;
http://www.marketwatch.com/story/traders-busted-after-enlisting-hackers-to-play-stock-market-to-net-100-million-2015-08-11.
2. *Schmidt M. S.* Hacking of Tax Returns More Extensive than First Reported // The New York Times. Aug. 17, 2015;
http://www.nytimes.com/2015/08/18/us/politics/hacking-of-tax-returns-more-extensive-than-first-reported-irs-says.html?_r=0.
3. Iran Confirms Stuxnet Worm Halted Centrifuges // CBCNEWS. Nov. 29, 2010;
http://www.cbsnews.com/news/iran-confirms-stuxnet-worm-halted-centrifuges/.
4. *Kovacs E.* Cyberattack on German Steel Plant Caused Significant Damage // Security Week. Dec. 18, 2014;
http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report.
5. *Nakashima E.* Hacking of OPM Databases Compromised 22.1 Million People // The Washington Post. July 9, 2015;
https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
6. *Lorra B.* ISIS's New Hit List: Over 1,500 Military Personnel and Goverment Officials Personal Information Leaked Online // Silent Soldier. Aug. 13, 2015;
https://silentsoldier.us/2015/08/13/isiss-new-hit-list-over-1500-military-personnel-and-government-officials-personal-information-leaked-online/.
7. *Setalvad A.* Demand to Fill Cybersecurity Jobs Booming // Peninsula Press. March 31, 2015;
http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.
8. *Thompson M.* Growing Cyberthreats Means More Jobs in US // CNBC. Aug. 7, 2015;
http://www.cnbc.com/2015/08/06/growing-cyberthreat-means-more-jobs-in-us.html.