Penetration Testing on Virtual Environments

Teresa Guarda
Universidad Estatal Peninsula de Santa Elena - UPSE
La Liberdad
Santa Elena
Ecuador
tguarda@gmail.com

Walter Orozco
Universidad Estatal Peninsula de Santa Elena - UPSE
La Liberdad
Santa Elena
Ecuador
worozco@upse.edu.ec

Maria Fernanda Augusto
Universidad Estatal Peninsula de Santa Elena - UPSE
La Liberdad
Santa Elena
Ecuador
mfg.augusto@gmail.com

Giovanna Morillo
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
giovi.morillog@gmail.com

Silvia Arévalo Navarrete
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
smarevalo@espe.edu.ec

Filipe Mota Pinto
Instituto Politécnico de Leiria
Leiria, Portugal
fpinto@ipleiria.pt

ABSTRACT

Since the beginning, computer systems have faced the challenge of protecting the information with which they work, and with the technological development, computational security techniques have become more complex to face the potentials attacks. Currently we are facing a war game with the usual two sides, attackers and defenders. The attackers want to have complete control over the systems. In is turn, defenders virtualized systems to maintain the resources safety in case of attack. The attackers have also developed increasingly sophisticated techniques to break such protections, being necessary to anticipate such events, which may be achieved through the application of preventative measures. This may be done by simulating Penetration Testing (PT). PT is an attack on a computer system, using a set of specialized tools that looks for security weaknesses, which eventually may have access to computer's features and data, allowing the discovery of such evidence vulnerability. Virtual Environments have a higher exposure to cyber-attacks. The aim of this paper is propose a framework to provide guidelines for Penetration Testing in Virtual Environments.

CCS Concepts

• Security and privacy → Virtualization and security → Penetration Testing → Trust frameworks.

Keywords

Penetration Testing; Virtual Environments; Vulnerability; Virtual Machine; Hypervisors.

1. INTRODUCTION

According data breach statistics from Verizon's (2016), 63% of confirmed data breaches involved weak, default or stolen passwords; 95% of confirmed web app breaches were financially motivated; 97% of breaches featuring stolen credentials leveraged legitimate partner access; 90% of Cyber espionage breaches capture trade secrets or proprietary information [1].

In attacks against ecommerce servers, web shells are used to access the payment application code and capture user input. The degree of sophistication of cyber-attacks has accompanied the rapid technological evolution.

Many cyber-attacks organizations can be avoided, and for that it is necessary to use appropriate security strategies. With these results, we still should be concerned, data security for virtualized servers is imperative [2].

Based on the principle that prevention is the best defense, penetration testing is a preventive activity that allows determines if the information is secure [3].

Penetration Testing allow testing computer security, to assess the level of security of the technological infrastructure and make the necessary corrections. For several years, it has been found that with this type of testing, it´s possible discover security weaknesses that compromise critical assets of organizations.

Although, it is necessary to have great knowledge and experience to perform penetration testing, this type of test is pertinent to large and small organizations with different technological infrastructure. The depth of penetration study can be applied even in equipment for personal use, and will depend on the required needs in respect of security controls to prevent unauthorized access.

To facing the scaling of applications and services required, organizations have focused on virtualization to optimize computing resources, and according to safeguard the security, it is necessary to investigate PT targeted for virtual environments, and this concern looking comply with this research have focused on virtualization to optimize computing resources, and according to safeguard the security, it is necessary to investigate regarding penetration testing targeted for virtual environments, and this concern this concern seeks to fulfill this research.

In this paper, we assume the perspective of the defender, who is trying to defend the virtual environment from the attackers wishing to execute malicious code. In the 2nd section is made a global exposure of virtual environments. The 3th section describes the penetration testing and their use. Finally, in the 4th section we propose a framework for penetration testing in virtual environments, which we hope will be an aid to help the defenders protect virtual systems from the attacks to which they are exposed. In the last section, the final considerations are presented.

2. VIRTUAL ENVIRONMENTS

System virtualization is the use of a software layer called Hypervisor, or Virtual Machine Monitor (VMM) that surrounds an operating system, and has the behavior that would be expected from physical hardware. For system virtualization, these virtual environments are called Virtual Machines (VM's), which operating systems may be installed.

CINS '16, December 28-31, 2016, Kuala Lumpur, Malaysia.
© 2016 ACM. ISBN 978-1-4503-4796-9/16/12□$15.00

DOI: http://dx.doi.org/10.1145/3026724.3026728

Virtual environment, it’s a tool that allows to run several different virtual machines within the same physical hardware, allowing a better use of the equipment, further considering that for a better management and network security is set one machine for each service in these networks. Using virtualization in a physical machine it´s possible creates several virtual machines (VM’s) separately to execute the same separate services as usual [4]. Then, virtualization creates a new environment, in which virtual machine systems is connected via virtual network interfaces, and via virtual routers, virtual switches and crossing virtual network. Virtualization also introduces a Hypervisor layer, this layer is a virtual machine manager (VMM) [5].

Virtualization has several advantages [6,7,8,9], such as: the costs reduction, when using this type of solution, it´s possible purchase a fewer physical equipment, for installation of the systems; a better management of servers with fewer people to carry out this control; OS flexibility, because it can be used in different operating systems in a simple and fast way; and a better use of resources, usually when network services are configured, the physical machines are not used to full capacity, and if we use virtualization, it is possible further explore the ability of the equipment; and is easier to upgrade, both the system and hardware, as well as the backup of the machines.

There are some confusion between virtualization and cloud computing, because both working together to provide different types of services, as is the case of private clouds. Virtualization and cloud computing are strictly connected for the reason that the major hypervisor vendors are directing all attention to cloud computing, to promote the adoption of private cloud computing.

3. PENETRATION TEST

Nowadays, many organizations are using web applications to maintain their value chain with customers and suppliers. These applications store valuable information, and may be the target of attacks by unknown malicious users, and the price of these attacks can be dramatic for the organization [10].

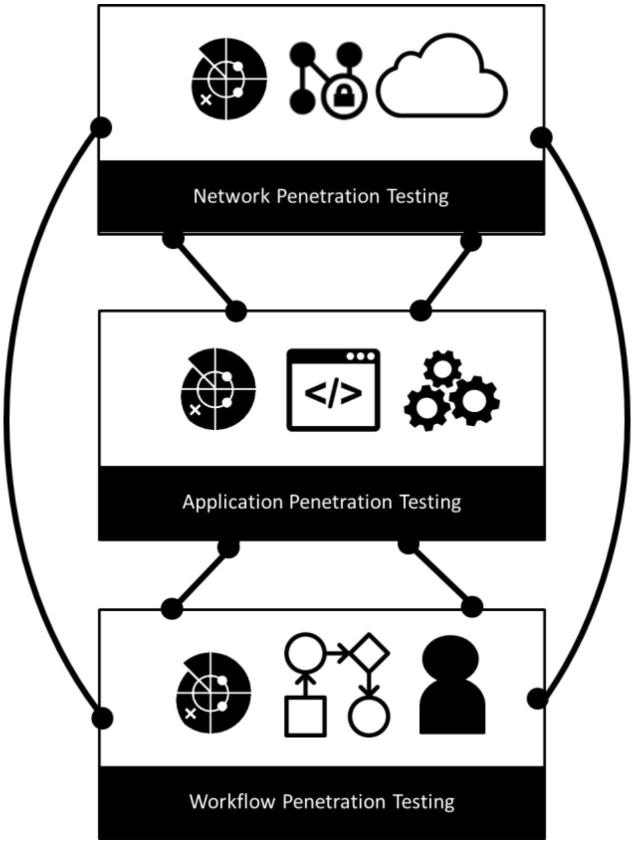
With the mass use of computers and access to internet service, it has made users commit computer crimes voluntarily or involuntarily, but authorities have not solved this problem by lack of infrastructure, equipment and highly qualified personnel.

The tools available to perform Penetration Testing have different degrees of complexity, and the management of some of them can be a challenge to the intelligence and sagacity of the attacker, also known as pen-tester. Among these tools, is possible refer, port scanners, complex algorithms to decipher passwords, intrusion systems brute force, network sniffing tools and firewalls penetration, as well as vulnerability scanning tools web applications and others.

A Penetration Testing, inform also known as Pen Test, is the intentional attack on a computer system, conducted with the objective to look for weaknesses in their security, thereby achieving access to the computer system features and data [11]. A Pen Test is not an easy task, and requires a solid and deep knowledge of the technologies involved in systems, applications and services as well as an optical and extensive experience in the behavior of various operating systems. These techniques used by Ethical Hacker can explore vulnerabilities in the system designed to meet the security flaws preventively, through the vulnerability analysis that are used to penetrate the system. Being the Ethical Hacking, the professional that exploits existing vulnerabilities in the system of "interest", using intrusion tests that verify and evaluate the physical and logical security of information systems [11,12,13]. Ethical hacker is a computer expert professional who is legally allowed to hack a computer system with the objective to protect from the criminal hackers, identifying the vulnerabilities and risks of a system and suggest how to mitigate them.

Some toolkits are highly regarded for the efficiency of their tools, and have been used in penetrations in high-level systems, which is their time were considered impregnable fortresses. Some of these kits are made available in CD format or ISO LIVE, and the tools are already built and installed on a bootable easy distribution operating system. Some tools are free and open source, others not, but powerful in both cases.

Penetration testing acts on three areas: network, application and system workflow (see Figure 1). The three areas are interrelated and share a common goal, identify systems vulnerabilities and risks exposures. In the case of network, all physical structure will be tested to identify breaches and treats that can create vulnerabilities and risks. Application Penetration Testing, include testing all the logical structure of the system, simulating a real attack that the efficiency of applications security. In the last area, all tests are designed for the workflow of the organization, and test the ability of the organization to prevent unauthorized access to its information systems [14].


Network Penetration Testing
Application Penetration Testing
Workflow Penetration Testing

Figures 1. Penetration testing acting areas.

Penetration Testing is organized into three categories: black-box, white-box and gray-box. In the 1st category, black-box, the pen tester has no knowledge of the system; he makes the job simulating an external attacker. On the other hand at 2nd, white-box pen tester has knowledge of system operation, at physical and logic level. Pen tester represents an attacker who has relevant information before attacking the computer system. The last category, gray-box, pen tester simulates be an internal employee, with username and password will find vulnerabilities by internal users. These categories allow testing all the logical structure of the system by a real attack simulation.

Penetration Test, allow testing information security to assess the level of security of the technological infrastructure and make the necessary corrections [15].

For several years now has been proven that with this type of testing, it´s possible discover security failings that compromise critical assets of organizations. Even though it is necessary to have great knowledge and experience to perform PT, this type of test is applicable to both large and small organizations with different technological infrastructure. The depth of penetration study can be applied even in equipment for personal use; and will depend on the required needs in respect of security controls to prevent unauthorized access.

Organizations facing the scaling of applications and services required, having focused on virtualization to optimize computing resources, and according to safeguard the security, it is necessary to investigate regarding PT targeted for virtual environments, and this concern seeks to fulfill the present research.

4. PENETRATION TEST FRAMEWORK

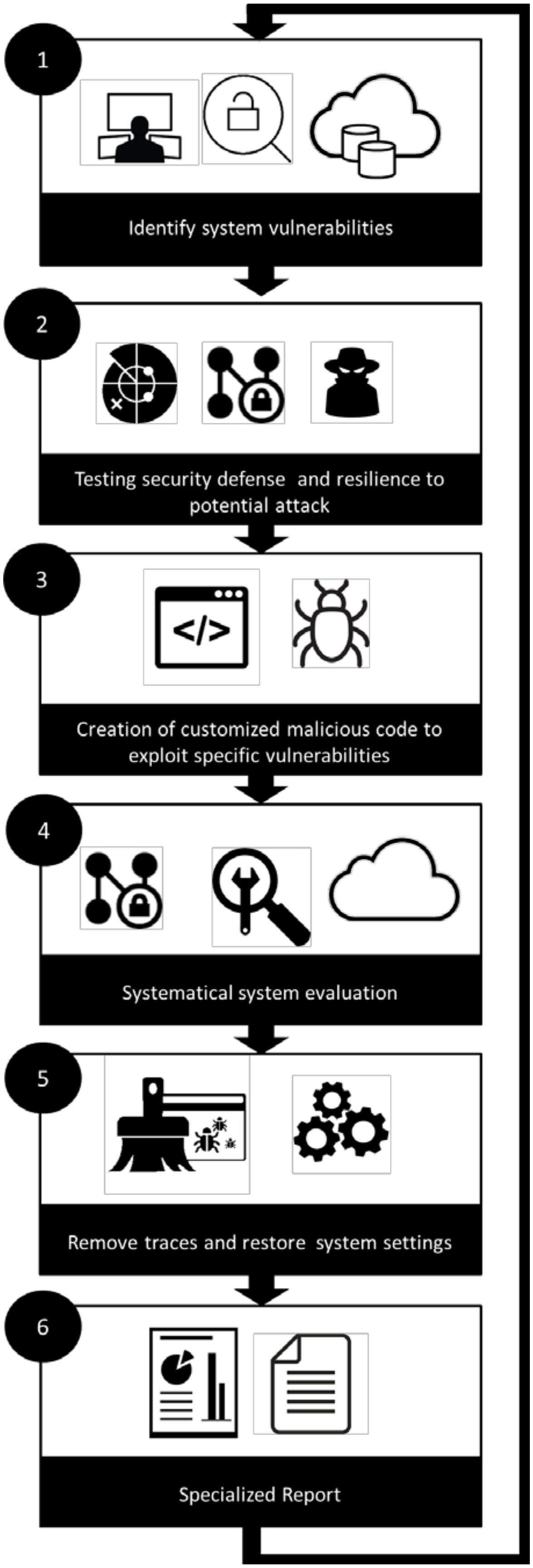
Unfortunately no system is hacker proof, then, one of most critical element of cyber defense is testing systems timely against most recent intrusion techniques. The virtualization in a public server increases significantly the risks of data breach, and is difficult identifying the attacker in this type of environment. In this scope, penetration testing on Virtual Environments (VE) permits the discovery of real risks within the VE, and suggests the methods and costs to mitigate the threats and breaches, providing an action plan for issue resolution; improves the overall protection system, and create a useful and a comprehensive security system report.

Penetration testing or Ethical Hacking is a deliberate search for potential system vulnerabilities using attack techniques [16].

Although the PT cost, they can be a profitable security investment [17]. A penetration test should satisfy some skills to be useful for organizations; need to be realistic, repeatable, reliable and reportable [18] . A PT should satisfy four R skills to be useful for organizations: must identify system vulnerabilities and update intrusion techniques (realistic); should include all risk exposure and mitigate weaknesses (reliable); the same test can be performed several times (repeatable), and all actions should be logged, allowing creates a useful, reliable and meaningful documentation, with findings and recommendations (reportable).

Based on these four skills, we will present a framework to provide guidelines for Penetration Testing in Virtual Environments.

The proposed framework is structured in six related phases; enabling several iterations in its life cycle, allowing mitigates attack vectors in a more effectively way (see Figure 2): (1) Identify all system vulnerabilities; (2) Testing effectiveness of security defenses and resilience to potential attack; (3) Creation of malicious customized malicious code to exploit specific vulnerabilities; (4) Systematical system evaluation; (5) Remove traces and restore system settings; (6) Specialized report.


1
Identify system vulnerabilities
2
Testing security defense and resilience to potential attack
3
Creation of customized malicious code to exploit specific vulnerabilities
4
Systematical system evaluation
5
Remove traces and restore system settings
6
Specialized Report

Figures 2. Penetration Testing framework.

In the 1st phase it's vital to identify all system vulnerabilities, and it is critical that any weaknesses or vulnerabilities in organization systems are found and mitigated before they are exposed to a cyber-attacker.

Immediately afterwards (2nd phase), the effectiveness of security defenses and resilience to potential attack will be tested. To do this, will be necessary to use a set of several tools (manual and automated), for scan, explore and test all systems (information system, infrastructures, networks).

Thereafter (3th phase), based in system evaluation outcomes, it should be selected the suitable set of attack vectors, and created malicious code to simulate attacks, allowing exploit vulnerabilities.

After that, in the 4th phase, it will be necessary to perform a systematical system evaluation. The system evaluation deals with several hundred of possible internal and external vulnerabilities, and at the end of this process, the results are categorized, the breaches analyzed and the solutions mapped. The PT, use automated and manual techniques, being these very similar with the techniques used by hackers, and will be scan for vulnerabilities, detecting and exploiting system potential entry points, revealing its weaknesses.

The next step (5th phase), based in last phase outcomes, traces will be removed, and configuration and system settings will be restored. Finally, in the 6th phase, the security report will be held. The document should include the definition of the scope of project, the risk analysis, the exposure to vulnerabilities, the degree of criticality and the impact of vulnerabilities in the organization, specifying critical alerts, detailing all critical vulnerabilities and mitigation measures to be implemented. All actions should be logged, allowing creates a specialized meaningful documentation, with findings and recommendations.

5. CONCLUSION

Virtualization with regard to security, if well implemented, deployed, monitored, and managed can offer security advantages, but a failure in any one of these can lead to disastrous results.

Penetration Test is a vital service that levered on a established methodology, that use a variety tools to systematically identify system vulnerabilities and weaknesses, analyzing breaches and mapping solutions, allowing mitigate attack vectors in more effectively way. The value of penetration testing depends from the use of the latest threat information and contextualization of these with the business. Penetration testing is particularly valuable for the maintenance of security of the virtual environments.

There are several security considerations to keep in mind in virtual environments, ranging from the hypervisor configuration, to the security measures and network storage, without neglecting the virtual machines. The naturally mobile nature of the virtualized environment requires security to travel with the virtual machine. Encryption and access control are of the greatest importance to protecting the VM and its data inside the data center. To expedite this situation at preventive level, and consequently at the security level, in the very near future PT should be made available as a service. In this context, all actors of virtualization can profit from PTaaS, from the cloud provider to the system owner, also including the ethical hacker, promoting the global security of virtualized environments.

6. REFERENCES

[1] VERIZON'. *Data Breach Investigations Report (DBIR)*. 2016.

[2] Furfaro, A., Piccolo, A., and Saccà, D. SmallWorld: A Test and Training System for the Cyber-Security. *European Scientific Journal, ESJ*, 12(10) (2016), 130-145.

[3] Yeo, J. Using penetration testing to enhance your company's security. *Computer Fraud & Security* (Apr. 2013), 17-20.

[4] Mihai, I. C. Penetration Tests on Virtual Environment. *Int'l J. Info. Sec. & Cybercrime*, 1(37) (2012).

[5] J. MICHAEL BUTLER;ROB VANDENBRINK. *IT Audit for the Virtual Environment*. SNAS, 2009.

[6] Morariu, O., Borangiu, T., and Raileanu, S. vMES: virtualization aware manufacturing execution system. *Computers in Industry*, 67 (2015), 27-37.

[7] Shkurkin, D., Novikov, V., Kobersy, I., Kobersy, I., and Borisova, A. Investigation of the scope of intellectual services in the aspect of virtualization and information economy of modern Russia. *Mediterranean Journal of Social Sciences*, 6(5 S3) (2015), 21-29.

[8] Ying-chun, Z. H. A. O. Application of Desktop Virtualization in the Library [J]. *Information Science 2*, 016 (2012).

[9] Hale, K. S. and Stanney, K. M. *Handbook of virtual environments: Design, implementation, and applications*. CRC Press, 2014.

[10] Halfond, W. G., Choudhary, S. R., and Orso, A. Penetration testing with improved input vector identification. In *In 2009 International Conference on Software Testing Verification and Validation* (2009), IEEE, 346-355.

[11] Krutz, R. L. and Vines, R. D. *The CISSP and CAP Prep guide*. Wiley, 2007.

[12] Henry, K. Penetration Testing: Protecting Networks and Systems. *IT Governance Publishing* (2012).

[13] Allsopp, W. *Unauthorised Access: Physical Penetration Testing For IT Security Teams*. John Wiley & Sons, 2010.

[14] Hydara, I., Sultan, A. B. M., Zulzalil, H., and Admodisastro, N. Current state of research on cross-site scripting (XSS)–A systematic literature review. *Information and Software Technology*, 58 (2015), 170-186.

[15] Sridhar, S., Hahn, A., and Govindarasu, M. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1) (2012), 210-224.

[16] Petukhov, A. and Kozlov, D. *Detecting security vulnerabilities in web applications using dynamic analysis with penetration testing*. Moscow State University, Computing Systems Lab, Department of Computer Science, Moscow, 2008.

[17] Böhme, R. and Félegyházi, M. Optimal information security investment with penetration testing. In *In International Conference on Decision and Game Theory for Security* (2010), 21-37.

[18] Dimkov, T., Van Cleeff, A., Pieters, W., and Hartel, P. Two methodologies for physical penetration testing using social engineering. In *In Proceedings of the 26th annual computer security applications conference* (2010), 399-408.