International Journal of Advances in Software Engineering & Research Methodology– IJSERM
Volume 2: Issue 2 [ISSN : 2374-1619]
Publication Date : 30 October, 2015

Penetration Testing in Online Gaming Industry

A S M Mohiuddin, Dilshad Ara Hossain, Munia Zaman Mumu, S M Salim Reza

***Abstract*— Online gaming is getting quite an attention in recent times. Nevertheless, the technical marvels that feed the collective hunger of the gaming industry is need of higher security. In fact, the tournament organized by valve for Dota2 (An online game) has total prize pool over 10million dollars (more than cricket world cup). Penetration testing is widely used to audit the security protection of information. It employs the same or similar techniques to those used in a genuine attack. Penetration test at its very center aims at an "illegitimate acquisition of legitimate authorization". This paper aims to discuss about penetration testing and how it can be used in online gaming industry to make it a safe and reliable zone for the professionals and also for the amateur players.**

Keywords*— *Penetration testing, Ethical hacking, Security, Vulnerability, Online gaming

I. Introduction

In this age of technology, everything has gone cyber from calling a friend to transfer goods. One of the major industries in this cyber world is online gaming industry. Many computer gaming studios are now making game which can be played in online with another person. Moreover it has now become a true sport because of the huge money involvement in these game's tournaments. Even South Korea made a proposition to the IOC to make some of the e-sports an Olympic Games event. But where there are cyber related something's, there are hackers. These malicious people will do anything for their personal benefit. Even in gaming industry server gets down, spam message comes to the client, password gets cracked and even account gets taken over by these hackers.

A S M Mohiduddin
Undergraduate Student
Military Institute of Science and Technology
Dhaka, Bangladesh

Dilshad Ara Hossain
Dhaka, Bangladesh

Munia Zaman Mumu
Dhaka, Bangladesh

S M Salim Reza
Assistant Professor, Faculty of Science & Technology, Bangladesh University of Professionals (BUP)
Dhaka, Bangladesh

Most people use real money in their gaming clients to buy gaming goods and thus it creates a major problem for them. Thus it is very much important for penetration testing in gaming industries. Not it only reduces the risk of getting hacked, it also exploits much vulnerability to the owner and thus he can take proper measures to fix those leakages. Objectives of a penetration test may vary and can be categorized using some general aims such as Identifying vulnerabilities and improving the security of technical systems as well as of the organizational and personnel infrastructure [1]. This paper analyses how we can do these penetration testing and how it should be used in online gaming industry.

II. Penetration Testing

Basically penetration test is referred to as a test to find out the system's vulnerabilities and making the system secure. Most of the time, we don't think about the security of the system. As a result, we pay the price when our security is breached by the malicious hackers. But now a days, everything has gone cyber so it's easy for hackers to penetrate the system and get benefit from it. So, penetration testing is very much needed in corporate sectors as well as many other industries to secure its confidential data. In penetration testing, it uses the similar method of a real hacker to exploit vulnerabilities. Thus it can have serious effects if it's not performed correctly. It might crash the whole system. Penetration test at its very center aims at an "illegitimate acquisition of legitimate authorization"[1].

III. Benefits of Penetration Testing

There are many benefits of penetration testing of a system. Some of them are given below:

- It can intelligently manage vulnerabilities
- Avoid the cost of network downtime
- Meet Regulatory Requirements and avoid fines
- Preserve corporate image and customer loyalty [1].

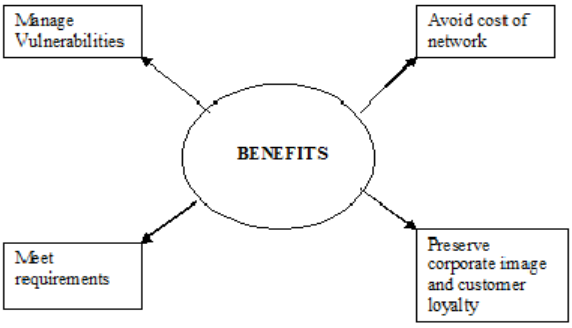

Fig : Benefits of Penetration Testing

SEEK DIGITAL LIBRARY

IV. Types of Penetration Testing

A. External Testing

- When a penetration test is conduct from outside of the system's network, it's known as external testing. It's the best way to find vulnerabilities from outside and thus prevent the outsider attacks. Basically it emulates the style of a real hacker and thus tries to find vulnerabilities from external sources. The goal here is to find the weaknesses in the system not to exploit them. External penetration testing's target is mainly attack the organization's externally visible servers like domain name server, email server, web server, firewall etc [1]. It finds that if the outsider attacker can get access to any of those servers by using various tools and if so then how much access they get. Then they report it to the corresponding in charge of the organization. The penetration tester may fix these vulnerabilities if he/she has permission from the corresponding organization.

B. Internal Testing

- When a penetration testing is hosted inside of the organization's network then it is called internal testing. It basically imitates the actions of a malicious user or employee which have access to a certain level of confidential information that might get the company into big losses if it goes into wrong hands. It designed to find weakness in internal networks like workstations, network equipment [1]. Internal Testing's main aim is to find how a malicious user can get access to valuable information on the system and how much access does he get when accessing as an employee.

C. Other types of Testing

There are other kinds of testing. They are given below:

- Black Box Testing: In this technique, the penetration tester has no knowledge about the organization's network system. He has to use penetration testing and social engineering to gain knowledge about the network system. It's basically how a hacker or a cracker basically attacks the system. It's one of the best ways to test the system's vulnerabilities. But it's very time consuming because initially having zero knowledge.

- White Box Testing: In this technique, the penetration tester completely knows about the system's network. Thus he can focus on only finding the vulnerabilities of the system. It's not a complete test because the tester knows all the information. Basically it needs for to do fast penetration testing.

- Gray Box Testing: In this technique, the penetration tester has some knowledge about the system's network. Basically he works in this method like an employee of the organizations. He has been given an account and standard access to the network. Thus he needs to find vulnerabilities from that point [4].

V. Phases of Penetration Testing

- The Pre-Attack Phase: In this phase the main objective of the penetration tester is to gather knowledge of the organization's network as much as possible. This is the phase to investigate and explore the network related information [1]. One of way to investigate is reconnaissance. It might be active or passive, doesn't matter. Another way to gather information is dumpster diving. Most of the organizations put some information to the trash. The testers can check the trash can and may find information about the network.

- The Attack Phase: Basically in this phase, the penetration tester tries to attack the system using information gathered from the pre-attack phase. There may be several weakness or vulnerabilities in the system but attacker need only one weakness to breach the system [1].

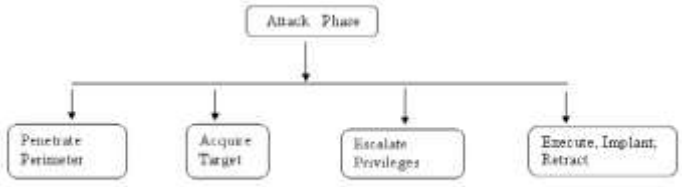

Fig : Attack Phase Stages

- The Post-Attack Phase: This is phase where the penetration tester returns any modification to the pre-attack state. The longer the system remains compromised the longer the attacker can acclaim credit for owing the system [1]. Thus the tester needs to tell these vulnerabilities to the organization. Thus they can take proper action for it.

VI. Using Penetration Testing in Online Gaming

- Client/Server Communication Vulnerability Testing: The penetration tester can check the vulnerabilities between servers to client communication in gaming. It's very important in gaming that the commutation do not get interrupt in games, otherwise it'll create a no playful environment. This year the Dota2 Asian Championship got interrupted quite a few times because of poor server to client communication.

SEEK DIGITAL LIBRARY

- Client-side exploit discovery: The penetration tester can also exploit the client side vulnerabilities by using gaming clients. Steam, Game Rangers is a few examples of game clients. People play various games using those clients in their server. If a penetration tester can find some vulnerability then he or she can tell it to the game organization. Then that organization can warn the user to fix the vulnerabilities to get better access.

- Discovery of potential weaknesses to denial of service attacks: The denial of service attack is one of the most dangers attack on a gaming client, in or off of a game. This attack is basically floods the server with fake requests. Thus the server gets overloaded with request and crash. In gaming it's very important to get server up all the time 24*7. Thus they need penetration testing to discover any weaknesses for DoS attack.

- Code review and vulnerability analysis: If the organizations give permission to the penetration tester that he can check and review the code of the client application and server application then he can check for vulnerabilities in it. In this case obviously the penetration tester should need basic app development skill.

- Web application vulnerability assessment: The penetration tester can also check the web application's vulnerability of the organization. Most of the gaming organizations have web application also. So. It's necessary to do penetration test on it every month.

- Infrastructure security review: The penetration tester can give a whole infrastructure security review of that gaming organization. The tester uses various tools like network analyzer and sniffer to detect unwanted IP accessing and thus can block that path to secure the gaming network.

- Payment security testing: Now most of the online gaming has purchase options in it. Thus users can buy goods to use it on game. Some gaming clients have their own wallet. So, user needs to put money in the wallet by using his bank account or credit card number. Thus the penetration tester need to check if the bank account/credit card number is valid and also if it's the users or not. If it's valid then the credit card number should be stored in a secure server for further purchase. If it's invalid then the users account should be blocked for a day or two, just to give him a fair warning.

- Spamming and Phishing Reviews: Many times users get spam message in their gaming client's chat. Sometimes it offers valuable in game products that are very rare to find. It's basically the attacker trying to hack that users account to get their stuff, credit card number and other kinds of information. When the user click on the link, the hacker gets access to that users account. Then he might change the user's password, get access to user's bank account and might steal money from that. So, it is user's duty to not to click on these link as well as penetration tester should check for spam message, if found one, block that account temporarily and tell the organization to take them proper action for it.

VII. Limitation of Penetration Testing

- **Post Development**: In penetration testing if security flows originate after the development, then it is costly to fix it.
- **Manual, one-time Audit:** Deception of specialized manual effort required for the test is hard.
- **Limited Range:** They have a limited range of testing project. Many organizations cannot test everything because of resource limitation. Penetration testers test those elements of the client's infrastructure that are deemed the most vital.
- **Skill of Penetration Testers:** Mainly the quality of a test depends on expertise and diligence. Without this requirement, test results get less measurable, reliable and assessable as they cannot be consistently reproduced. Experienced penetration testers also have some limits, focusing power and having less expertise in others [1].

VIII. Penetration Testing Requirements

Penetration testing is an inclusive method to test the complete, integrated, operational and trusted computing base that consists of hardware, software and people. There are many organizational issues that are necessary to be focus before a penetration test or security review. This necessity can include legal and contractual issues. There are also some technical requirements for penetration test like:

- Range of IP addresses in which the test to be escort.
- Time limitations.

SEEK DIGITAL LIBRARY

- Source of IP addresses that is targeted part of test.

Theoretically there are a number of ethical and competency issues that penetration testers face in conducting an assessment, from testing systems or protocols not explicitly included or excluded from a test, to significant omissions that cloud possibly be disastrous to an organization. Penetration testers are ethically bound and affiliated by the customer's need. At the same time they should ensure that the penetration test is correct and does not misguide [5].

IX. Future Hope

At present, penetration testing can only be used by the organization or industry. They use it to secure network that check vulnerabilities between server and customers communication. This organizations help customers in terms of

- Client/server communication vulnerability testing
- Client benefits discovery
- Find possible weakness to denial of service attack
- Review basic physical and organizational structures and facilities for securely operations
- Provide payment security testing
- For information security reviews spamming and phishing

X. Conclusion

A penetration test is carried out with the intent of finding errors. Therefore, it is very much needed in online gaming industries because of the faulty servers. But it must not be overlooked that doing a penetration test, doesn't mean that the system is totally secured. Some part of the system or network must be secured but attackers always try to find newer ways to penetrate the system. So, the organization should try to test their system and networks at least once per week. As gaming server should always be open, in gaming, it's essential to do penetration test everyday while simultaneously running the servers.

References

[1] Ethical & Penetration Testing: An Overview by AkankshaBansal Chopra, Assistant Professor, Department of Computer Science, Shyama Prasad Mukherji College (University of Delhi),

[2] An Overview of Network Penetration Testing by Chaitra N. Shivayogimath, PG Student, Dept. of ECE, AMC Engineering College, Bangalore, Karnataka, India

[3] Online Gaming Security (http://www.senet-int.com/services/online-gaming-security/)

[4] An Overview of Penetration Testing by Aileen G. Bacudio, Xiaohong Yuan,Dept. of Computer Science, North Carolina A&T State University, Greensboro, North Carolina, USA&Bei-Tseng Bill Chu, Monique Jones, Dept. of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, North Carolina, USA

[5] Penetration Testing and Vulnerability Assessments: A Professional Approach by KonstantinosXynos, University of Glamorgan. Iain Sutherland, University of Glamorgan. Huw Read, University of Glamorgan. EmlynEveritt, University of Glamorgan. Andrew J C Blyth, University of Glamorgan

About Author (s):

A S M Mohiuddin is currently pursuing his B.Sc. (Eng.) in Computer Science and Engineering from Military Institute of Science and Technology. Mirpur Cantonment, Dhaka, Bangladesh.

Dilshad Ara Hossain is a CSE graduate from Bangladesh. She worked as ICT Teacher in GCSE Level on Dhaka. Her research interest includes ICT, Telecommunication, Electronics, Cyber Security and International Cyber Law.

Munia Zaman Mumu has completed her B.Sc Engg in CSE from University of Asia Pacific (UAP). Her research interest includes server security, cloud security etc.

S M Salim Reza has been serving as Assistant Professor of the Department of ICT, Faculty of Science and Technology (FST) in Bangladesh University of Professionals, Mirpur Cantonment, Dhaka, Bangladesh

SEEK DIGITAL LIBRARY