Results of Penetration Testing on different Windows Client Operating Systems

Sushil N. Gawhale
Dept. of CS and IT,
Dr. B.A.M. University,
Aurangabad MS (India

Ramesh R. Manza
Dept. of CS and IT,
Dr. B.A.M. University,
Aurangabad MS (India)

Yogesh M. Rajput
Dept. of CS and IT,
Dr. B.A.M. University,
Aurangabad MS (India)

ABSTRACT
Windows operating systems are very popular among people from common men to specialists also. We will be working on some operating systems in this paper. People out of there often select windows operating system as importance among several others. So are our information and data secured? To answer this we make use of penetration testing on window client operating system and test various exploits on windows operating system by using the kali Linux Operating system. Try to exploit operating system. Penetration tests provide evidence that vulnerabilities do exist as a result network penetrations are possible as well as any workstation vulnerability. They provide a blueprint for remediation. Methodology include: discovery, enumeration, vulnerability identification, vulnerability assessment, exploitation and launching of attack, reporting, external penetration testing, internal penetration testing, legal issues before you start.

Keywords
Exploit, payload, Hacker, Structure hacking, unstructured hacking, Penetration Testing, Information Security.

1. INTRODUCTION
Vulnerability Assessment and Penetration Testing (VAPT) is a Systematic study of security position of Information systems. Vulnerability assessment is an on-demand result which makes it suitable to run tests over the Internet anywhere, anytime. It is a mixture solution which blends automated testing with security expert analysis. The unique technology classifies all thinkable attack courses. Vulnerability assessment suggestions fractional evaluation of vulnerabilities, actually testing for vulnerabilities done by penetrating barriers is useful assistant. As it identifies possible access paths missed by VAS. Penetration testing aka "pen testing" is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit [1].

Vulnerability assessment and penetration testing in the act of structured hackers. It is a process to copy all ways used by hackers to compromise a system. But with the difference is honestly structured hacker in deed so as to know in prior how a machine can suffer security breach attack. Created Virtual Environment for security purpose and can't harm to real-time workstation. To cover all of process of penetration testing also called pretesting, we will perform our test on various windows operating system like as a windows XP Professional 32bit, windows 7 Professional 64bit and windows 8.1 professional 64bit & Windows 10 professional 64bit Let see results of Penetration testing on them [3].

2. A BRIEF INTRODUCTION ABOUT CYBER SECURITY
Cyber Security, the most concerned topic in all our world, and the most concerned area in today's online world [4]. The vast number of oppositions were received about hacking acts. Peoples around there, using internet medium for most of their sort of stuff including business, communication, and fun have a fear of being observed or hacked by malicious users. So for our purpose we have used kali Linux open source live operating system (Attacker machine), in the Kali Linux tools like Metasploit, Armitage perform in Virtual Environment on several windows OS (Victim machine), VMWare workstation pro (Virtual Environment) used for a creating virtual Environment.

3. METHODOLOGY
A figure below shows the concept behind how working exploit and how will be Penetration Testing windows operating system.

In the penetration test we will be used two exploits first **windows/meterpreter/reverse_tcp** and second one is **exploit/windows/smb/ms08_067_netapi** this two exploits mostly used for penetrating windows operating system. But those exploit working on only without Antivirus victim system. If in victim machine having antivirus it will be detecting exploits

Exploit
Exploit is the piece code that allows the attacker to take advantage of the vulnerability.

Payload
A Payload is piece code or program that runs after the exploit is successfully executed.

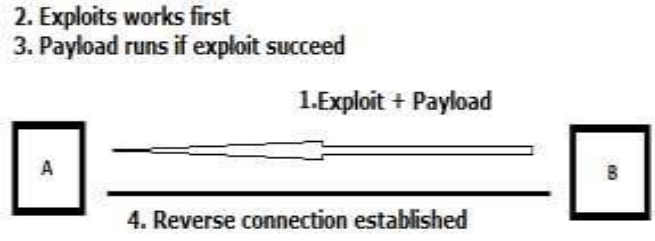

Fig.1. General Penetration Testing Process in network workstations

Hence, A is supposed to be a victim of B. So B will be our machine with Kali Linux operating system and A will be windows operating systems like windows XP, windows 7, windows 8.1 and windows 10. First a combination of exploit + payload is loaded onto a victim vicinity. Then exploit

comes into work, payloads starts its execution only if an exploit succeeds. Once an exploit succeeds [6], a reverse connection is established as per the use of **windows/meterpreter/reverse_tcp** exploit. Now, a time for action, we can do multiple tasks like data uploading & downloading, registry read/write operations, recording of keystrokes, taking snapshots, process migration and much more. Once the desired tasks are achieved we can aim high for privilege escalation.

4. WHO IS THE HACKER?

Several definitions and types of hackers are given below

Hackers are clever personality's persons with great computer knowledge about software, hardware as well as networking & servers also, hacking is interest to test their capacity by themselves. Some do it with well-planned policy to complete their incorrect purposes. To better recognize them, they are additional categorized into four groups. They are:

4.1 White Hat Hackers

White hat hackers are ethical hackers (Structured hacker) with some certifications such as CEH (Certified Ethical Hacker), LPT (License penetration tester) also called as a Structure hacker. These type of hacker create their own tools for implementing hacking and they break systems just for legal purposes. They also known as government lows of cyber forensic. Their main reason is to find vulnerability in the networks and repairing them. These type of hackers work with well-known businesses in securing their systems and defensive them against other hackers [3].

4.2 Black Hat Hacker

A black hat hacker they don't have any hacking certification but they hold good knowledge about hacking. These type of hacker one of the beginners or experts. They used tools created by structure hacker which are available in internet. They use their skills for negative purposes also this peoples told as unstructured hacker. They break into systems and networks either for fun or to gain some money by illegal means. Those person gain illegal access and destroy/steal confidential data and cause problems to their target & most of the time they don't know the consequences [4].

4.3 Grey Hat Hacker

A grey hat hacker person's combination of both hacker as structure hacker and unstructured hacker. A Grey Hat Hacker can top the internet and hack into a computer system for the sole purpose of updating the officer that their system has been hacked. They may offer to repair their system for a small payment. [5].

5. HACKING CAN BE DIVIDED INTO MANY PHASES

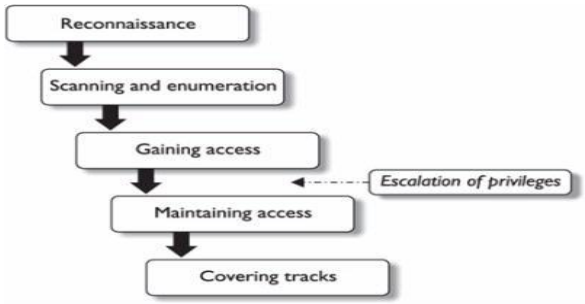

Fig.4 Process of Hacking

5.1 Reconnaissance (Information Gathering Or Foot Printing)

In this Reconnaissance (information gathering) so in this process hackers refers to gather more information as we can about target in previous to perform an attack. It can be more classified into two categories Active and Passive. Earlier includes information gathering with direct interaction like social engineering and the later without any direct interaction by searching news or public records.

5.1.1 Active Information Gathering

In active information gathering going one step further of passive foot printing, where we are actually reaching the system itself and have a very limited possibility of being discovered throughout the process (SEO) search Engine optimization & (AIS) Autonomous System number.

5.1.2 Passive Information Gathering

In passive information gathering basically in an non intrusion manner from a third party organization or a Network about the target

5.2 Scanning

Scanning is first action taken against target. In this phase, we use the information obtained from foot printing and move dipper into victim machine and network. Network scanned to determine which host are live and them more deep for more information. In this scanning section refers to scan for all the open ports as well as closed ports and even which services use victim also get vulnerabilities of victim using scanning the known vulnerabilities.

5.3 Gaining Control

In this process can be gained at Operating system and even network infrastructure. From normal access hacker can even proceed with decency increase.

5.4 Maintaining Access

In this process hacker struggles to retain its control finished target with entrances, rootkits. Collaborated workstations

5.5 Log Cleaning

This process also known as cleanup workstation. Remove all loaded executable, scripts, and temporary files from victim system. Return all replaced original values and system setting, application arrangement parameters if they were modified from system.

6. RESULT

As discussed earlier, we will be creating an attacker and victim scenario. An attacker will be our Kali Linux and victim will be any of the windows client operating systems. Well a simple penetration testing works in manner like:

1. Setting an exploit suitable for respective Operating System
2. Setting a payload according to need (we use Windows/Meterpreter/reverse_tcp)
3. Assigning LHOST and RHOST (LHOST: IP address of an attacker RHOST: IP address of a victim machine).
4. Throw an exploit command.

So in above steps we had a glance over a common steps on penetration testing. So what is new in this paper? A payload made by this process is somewhere detectable over many

machines which warns a user about it before its execution. So to avoid this case we actually wrap up these commands in a shell file along with syringe.exe. Syringe.exe has by default windows permissions so doesn't get detected. We used Kali Linux and various Operating System using the payload **windows/meterpreter/reevrse_tcp**. The results were shown in a table.

Table 1. Results

Operating System	Payload	Result
Win XP	Meterpreter/reverse_tcp	Breached
Win 7	Meterpreter/reverse_tcp	Breached
Win 8.1	Meterpreter/reverse_tcp	Breached
Win 10	Meterpreter/reverse_tcp	Breached

.

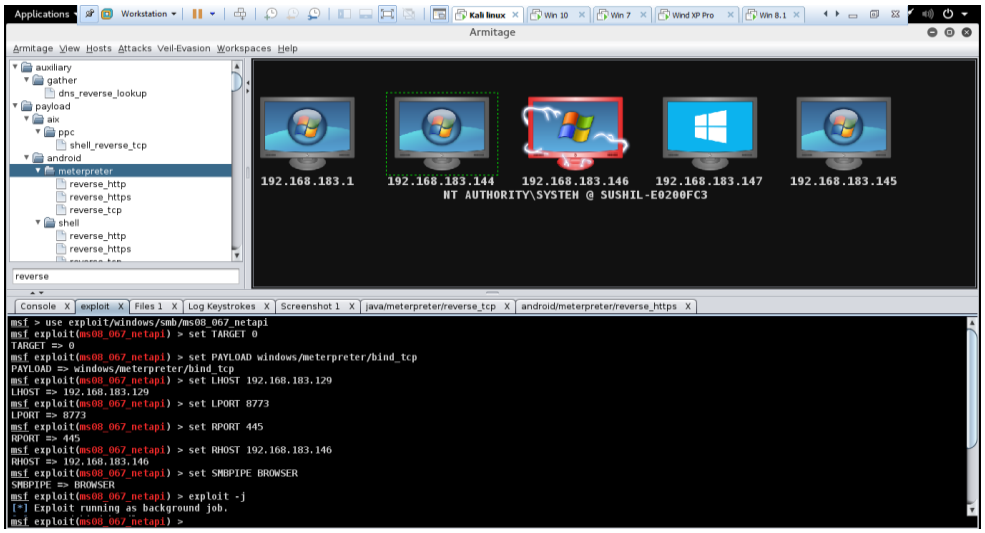

Fig.5. Hacking Implementation in virtual environment

7. CONCLUSION

Conclusion is accomplish all the features of structured hacker as well as an unstructured hacker It's currently must for all to hire huge methodology and in our public or private network used Firewall and Routers for filtering every packet and detect the IDS (Intrusion detection system) & IPS (Intrusion prevention system) to monitoring on network as well as securing our network. Structured hacker penetration on network for any vulnerability of our network for security purpose to avoid hacking we have tested four windows operating systems which were being compromised with syringe utility

8. FUTURE SCOPE

We tried here payload not to get detected over it. But silent there is a problem that it has its record shown in task manager area. So one should try in future to prevent this entry in task manager. We have tested five windows operating systems which were being compromised with syringe utility.

9. REFERENCES

[1] Vulnerability Assessment and Penetration Testing http://www.aretecon.com/aretesoftwares/ vapt.html

[2] Internet Crime Complaint Centre link: www.ic3.gov

[3] Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min; "Software vulnerability Discovery Techniques: A Survey" IEEE Conference Publication, DOI: 10.1109/MINES.2012.202, Page(s) 152-156, 2012

[4] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI:10.1147/sj.403.0769, Page (s): 769-780

[5] Bradley, Rubin "Computer Security Education and Research: Handle with care" IEEE Conference Publication, DOI: 10.1109/MSP.2006.146, Page(s): 56-59

[6] Prakash Chandra Behera, Chinmaya Dash "Ethical Hacking: A Security Assessment Tool to Uncover Loopholes and Vulnerabilities in Network and to Ensure Protection to the System", International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Special Issue May 2015.

[7] Robinson, S. "Art of Penetration Testing" Security of Distributed Control Systems, 2005. The IEE Seminar on Date of Conference: 2 Nov. 2005. Page(s): 71 – 76.

[8] Budiarto, R.,Sureswaran Ramadass "Development of penetration testing model for increasing security" Information and Communication Technologies: From Theory to Applications, 2004. 2004 International Conference on Date of Conference: 19-23 April 2004, Page(s): 563 - 564.

[9] Network Penetration Testing Expert "US-COUNCIL", link https://www.us-council.com/free-ebooks/NPTE-Student-Handbook/html5forpc.html.