Results of Penetration Testing on Various Operating Systems

Laxman Vishnoi
M.Tech(I.T.) Student,I.T.M. College
laxman.vishnoi@gmail.com

Vivek Shrivastava
Asst. Prof. (I.T.), I.T.M. College
viveks2001@gmail.com

Abstract: *Windows operating systems have been very popular among people from common men to professionals. We will be working on some very popular windows operating systems in this paper.*

People out there often choose windows OS as a priority among several others. So are our information and data secured? To answer this we make use of penetration testing.

Pentesting: *It is a process to imitate all ways used by hackers to compromise a system. But with the diference its is purely ethical in deed so as to know in prior how a machine can suffer security breach attack.*

In a sign, cyber security must be aided with quality issues and advancements. In a row, two more U.S. companies, McDonalds Corp. and Walgreen Co., revealed that they had been compromised along with U.S. media company, Gawker. Much of this hacked information was supposed to be provided by end customers when they used to sign up for online subscriptions.

The main objective of this paper is to cover core elements of process of penetration testing also called pentesting.

We will perform our test on windows XP, windows 7 and windows 8. Let see what are results of pentesting on them.

Keywords: *Hacking, Hacker, Ethical Hacking, Penetration Testing, Information Security.*

1. A Brief on Cyber Security

Cyber Security, the most concerned topic and the most concerned area in today's online world[3]. The vast number of complaints were received about hacking acts. People around there, using internet medium for most of their sort of stuff including business, communication, fun have a fear of being observed or hacked by malicious users.

So for our purpose we have used the tools like Backtrack 5 R3 (Attacker machine), several windows OS (Victim machine), VMWare workstation 9.0(Virtual Environment)

2. Main Concept

A figure below shows the concept behind Penetration Testing.

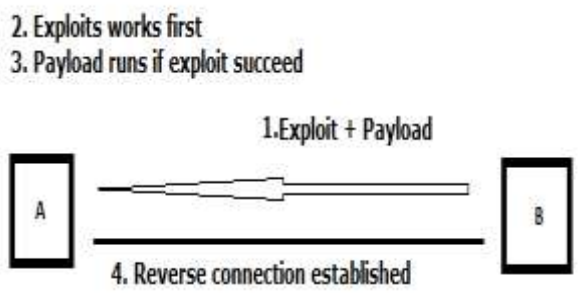
2. Exploits works first
3. Payload runs if exploit succeed
1.Exploit + Payload
A
B
4. Reverse connection established

Fig.1. *Penetration Testing Process*

Here, A is supposed to be a victim of B. So B will be our machine with Backtrack 5 R3 and A will be windows operating systems like xp , 7 and 8. 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 payload. Now, a time for action, we can do multiple tasks like data uploadi 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 privelege escalation.

Once when we start building notions about

3. Who the Hacker is?

Several definitions for hackers are given below :

- Hackers are capable individuals with extreme computer knowledge about software as well as hardware.

- For some notorious individuals, hacking is just an hobby to test their ability by themselves.
- Some do it with well planned strategy to complete their wrong intentions.

To better understand them, they are further classified into four categories. They are :

- Black Hat Hacker : Their deeds results into destructive activities. They are also known as crackers.
- White Hat Hacker : They are professional hackers. They use their skill for defensive purpose in purely an ethical way.
- Suicide Hacker : They are such notorious individuals who aim to bring down critical structure and even does not care about facing punishment.
- Gray Hat Hacker: They are the hackers who are mixture of both white hat and black hat hackers i.e. works both offensively and defensively[5].

Hacking can be divided into many phases :

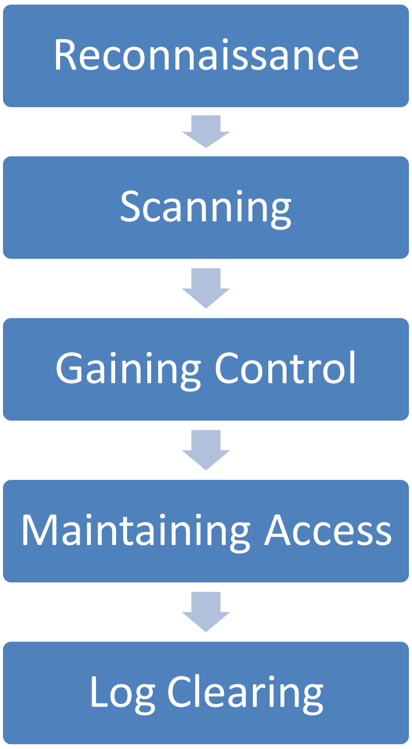

Fig.4 Hacking *Process*

3.1 Reconnaissance

It refers to gather as more information as we can about target in prior to perform an attack. It can be further classified into Active and Passive. Former involves information gathering with direct interaction like social engineering and the later without any direct interaction by searching news release or public records.

3.2 Scanning

It refers to scan for all the open as well as closed ports and even for the known vulnerabilities on the target machine.

3.3 Gaining Control

It can be gained at OS level, system level or even network level. From normal access hacker can even proceed with privilege escalation. It often includes password cracking, buffer overflows, DoS attack etc.

3.4 Maintaining Access

It is where hacker strives to retain its control over target with backdoors, rootkits or Trojans. Compromised machines can even be used as Bots and Zombies for further attacks.

3.5 Log clearing

It is also known as Daisy Chaining. To avoid being exposed or caught, a good hacker will leave no impressions of his presence. So he attempts to overwrite the system and application logs.

4. Experiment

As discussed earlier, we will be creating an attacker and victim scenario. An attacker will be our Backtrack 5 r3 and victim will be any of the windows operating systems chosen earlier. Well a simpe penetration testing works in manner like :

1. setting an exploit suitable for respective OS

2. Setting a payload according to need (we use windows/meterpereter/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 pentesting. 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.

5. Results

We used Backtrack 5 R3 and various OS using the payload windows/meterpreter/reevrse_tcp. The results were shown in a table.

Table 1. *Results*

OS	Payload	Result
Win XP	Meterpreter/reverse_tcp	Breached
Win 7	Meterpreter/reverse_tcp	Breached
Win 8	Meterpreter/reverse_tcp	Breached

6. Future Scope and Conclusion

Conclusion:

To conclude all the aspects of hacking as well as an ethical hacking. It is now must for all to hire methodology of an ethical hacking to avoid

To conclude all the aspects of hacking as well as an ethical hacking. It is now must for all to hire methodology of an ethical hacking to avoid hacking consequences. In prior, to expose all loopholes in a system to a broad network, it becomes crucial. We have tested three windows operating systems which were being compromised with syringe utility.

Future Scope:

We tried here payload not to get detected over it. But still there is a problem that it has its entry shown in task manager vicinity. So if someone goes deep into it, he can check it out there before downloading a malicious file. So one should try in future to prevent this entry in task manager.

To conclude all the aspects of hacking as well as an ethical hacking. It is now must for all to hire methodology of an ethical hacking to avoid hacking consequences. In prior, to expose all loopholes in a system to a broad network, it becomes crucial. We have tested three windows operating systems which were being compromised with syringe utility.

Future Scope:

We tried here payload not to get detected over it. But still there is a problem that it has its entry shown in task manager vicinity. So if someone goes deep into it, he can check it out there before downloading a malicious file. So one should try in future to prevent this entry in task manager.

hacking consequences. In prior, to expose all loopholes in a system to a broad network, it becomes crucial. We have tested three windows operating systems which were being compromised with syringe utility.

Future Scope:

We tried here payload not to get detected over it. But still there is a problem that it has its entry shown in task manager vicinity. So if someone goes deep into it, he can check it out there before downloading a malicious file. So one should try in future to prevent this entry in task manager.

References

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

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

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

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

[5] Wilbanks "When Black Hats are really white" IEEE Conference Publication, DOI : 10.1109/MITP.2008.146, Page(s): 64

[6] 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.

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