Vaibhav Shukla
MIS 5212
Advanced Penetration Testing Analysis Report 1 – Metasploit
Date-02/21/2017

Introduction

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.Its best-known sub-project is the open source. Metasploit Framework, a tool for developing and executing exploit code against a remote target machine

OBJECTIVE

The Objective of this analysis was to run a vulnerability scan to find the potentional vulnerabilities in a compromised system and then use metasploit to exploit any one of the vulnerabilities

Executive Summary

I conducted a basic network scan using the IP Address of metasploitable. Instead of running Nessus within Metasploit, I decided to run Nessus on my browser. After the scan completed, I exported the results into a '.nessus' file format then navigated back to Metasploit and imported the nessus file to be used for exploiting any of the vulnerability

I picked one the critical backdoor vulnerability "UnrealIRCd Backdoor Detection". This backdoor allows a person to execute any command with the privileges of the user running the ircd. The backdoor can be executed regardless of any user restrictions (so even if you have passworded server or hub that doesn't allow any users in). Unreal3.2.8.1.tar.gz file on mirrors has been replaced with a version with a backdoor (trojan) in it.
I used this exploit directly in the metasploit and used options command to know more about the way to exploit it. I loaded the exploit using the 'use' command, 'set' the 'RHOST', and entered 'exploit'. The exploit was successful, as I was given root access to the target's shell.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it

Conclusion

Metasploit can import vulnerability scanner data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation. The metaspolit is an effective tool to conduct the pen-testing .