Penetration Test: File Payload Attack

**Executive Summary**

Phishing is arguably the most popular attack method hackers use to compromise victims’ machines or systems. Several studies confirmed that most hackers deliver malicious codes and files via either email, social media, random computer systems’ locations, and so on. Metasploit, SET, MSF are among common tools hackers utilize to either break into computer systems or conduct penetration tests. The following is a demonstration of two forms of attack methodologies to compromise targeted machines. I utilize Metasploit to try maintaining access with a “File Uploading Backdoor” and “SET” to deliver a malware file, then break into my targeted machine.

**File-Upload Backdoor**

After launching Kali and Metasplloit, I begin by generating a reverse-connecting jsp shell to setup a payload listener. To complete this step, I run a “msfvenom” query and additional commands within which IP address and port are identified. Next, I upload another shell code to my targeted remote machine that supports jsp files. Considering that the file uploaded to the remote server, I follow-up with requesting the file in my browser and receive the shell. To finish the attack, I enter a couple more query lines in Metasploit with the intention to identify the hostname and additional computer systems information such as: IP address, default gateway, operating system and so forth. As I explain in my presentation, my exploit failed due to strong internet security protection implemented in the victim’s machine.

**Payload attack using SET**

I use SET to test another attack methodology. First, I select the social engineering attack by entering 1 after starting the social engineering tool. Secondly, I choose 9 as a powershell attack vector and 1 for powershell alphanumeric shellcode injector. The third step includes entering additional query codes such as: IP address, port, etc. I copied the root of my file path, open a new terminal in Kali, then past it there to enter. Lastly, I copy the next created file location, then past it again along with more query codes.

Now Metasploit is listening for the packet coming from victim’s machine once the attempt to open the payload file.

**Mitigation suggestions**

Several good measures can be adopted to protect a computer against payload or social engineering attacks. First, organizations and IT Security professionals should remember that similar hackers’ methodologies can be applied against them. Secondly, evaluate and test systems regularly. Also, make it a company culture to consider IT Security as a vital part of business practices.