Metasploit For Windows 7 32-bit 261l

I developed a python script to create the LocalSystem Service account on any vulnerable Windows machine. This script will make sure the newly created account is on a safe list, which keeps the computer from crashing when you try to run the exploit. Be warned that you MUST run this script on a computer that the malicious actor was able to successfully connect to (usually the victim) or on the same computer that is affected, otherwise the exploit will not function properly. Make sure that the meterpreter payload is used on the affected computer, as other payloads such as the one in this tutorial dont affect the service. net localgroup new-user Administrator /add This will create a user called new-user and add it to the Administrator group on this computer. Depending on the Windows version, the user will be set to log on automatically when you reboot your computer. Otherwise, you can run the following to make sure you dont lose access to your account in the event that the user fails to log on: net user new-user /active:yes Metasploit For Windows 7 32-bit 261l As mentioned in the instructions, to use the zzz_exploit script, we need a couple of python libraries (see the metadata for more on what these packages do). Simply installing the.pth file that is provided with the zzz_exploit will install both the mysmb and the creds tool from the Python Package Index (PyPI) from the same repository. Aside from the extra PATH variable, there is very little that is different when using a Windows based system to run Metasploit. Weve already come across a few things of interest, such as the 'rrun' utility, and the IPTABLES rules we just generated earlier. We would run into issues if we had to adjust the PATH for each'setup' or use 'rrun' directly when using the installed MSF handler for this particular exploit. After running the 'exploit' script, we can review the command output to verify the OS version of Windows 7:

To upload the script we use Metasploit Meterpreter VM Upload script. You can also use upload.rb. We will need to set the NET environment variable (fig 6) to host IP (or 0.0.0.0 if you dont care about where the script is executed). If you want to have the script executed privately then make sure you connect to the target machine from the host machine and execute it this way (fig 7). If you dont want to execute the script from the host you need to set the proper parameter to the command from the host (fig 8). To configure a TCP meterpreter handler. On the target machine create a meterpreter request with msfcli handle_tcp -j (fig 9). Metasploit has many pre-configured payloads for you which can be used for a variety of attacks. The payloads in this tutorial are mostly pre-configured for use in the password cracking contest. We can use passwd_crack payload which sends the chosen password to the target in clear-text via netcat. There are several other options to consider such as attack_tln which will deliver a unique TINFO (two step login) to the target. Another useful payload is hashcat to attack hashes. Once all these pre-configured attacks are available to you you are free to come up with your own; there are about 45 different exploits to choose from. # Select the attack you want to use /msfconsole auxiliary/analyze/passwd_crack_meta_windows_7 Metasploit For Windows 7 32-bit 261l Hash Suite is very flexible and will prompt for the right password to crack. At this point you should be in an interactive shell. Start by looking for malicious commands like ls -al or show active processes. If you see something that doesnt look like the user is doing anything, type onidle and press enter. The system will reboot and the user will have a session when the machine comes back up. The user wont be logged out of X, so this is one reason why you may need to look for malicious commands that will re-start the X session. Theres a possibility that the user could remove malicious code or kill the metasploit session. 5ec8ef588b