PenTest Lab Exercise Ex0c0 – Hiding in Plain Sight

Goal

Use a new PowerShell tool that gives meterpreter-like capabilities but is not caught by Windows AMSI.

Tasks

1. Sometimes even the best plans go wrong. Hank was sure he could get you to use one of the tools Veil, Invoke-Obfuscation, or Invoke-CradleCrafter to deliver a meterpreter executable to a machine running Windows 10. Now he's not so sure. Hank wants you to give it one last try on a machine where you don't have an administrator account.

   To do this, log in to Netlab and schedule an Ex0c0 lab.

2. Connect to `books`. Try to get access by using credentials you've already found. You can try to establish a remote desktop connection from `costumes` by running the MS Terminal Services Client (`mstsc.exe`), however, working from `costumes` may be hard. I recommend you install a chisel proxy and go through that straight to `books` using proxychains on rdesktop. Please understand that only certain users (domain or local) may be authorized to use `RDP` on `books`, so you may have to try several different users before you succeed. And beware: the domain for a local user is the host name (not some other host's name).

3. Hank wants you to test a Veil payload he generated earlier. This is stored in directory `/var/lib/veil/output/source/`. If the payload is a `.exe` or `bat` file, you can execute it at the command line in a windows `cmd` or `PowerShell` window. If you are using a Veil payload named `payload_name.`*xxx* correctly, before you execute the payload, you will start `msfconsole` and you will execute

   ```
   resource /var/lib/veil/output/handler/payload_name.rc
   ```

   which will start a handler for the meterpreter that the payload is delivering.

   Try running the payload and see if Windows AMSI detects it.

4. Hank may be disappointed by what you find, but he is never down and out. He knows that when there is a great need, the hacking community will provide. He heard about `r00t-3xp10it`'s `Meterpeter` project. (No that's not a misspelling.) `Meterpeter` is a tool with capabilities similar to the Meterpreter, but it does not depend on the Metasploit framework. It's primary selling point is that it provides a Command-and-Control (C2) framework that is not yet recognized by Windows AMSI. Thus, it can be delivered to and used on Windows hosts with impunity. You can find some information on its use in this (slightly outdated) article, meterpeter: C2 Powershell Command & Control Framework.

   Hank wants you to assess the utility of meterpeter by delivering it to books (if you can) and seeing if you can exfiltrate files using it. For the purposes of this assignment, Hank wants you to exfiltrate any file belonging to a user on books. If the files you find do not contain any sensitive data, there may be no finding of note, however, you should still report what you find to Hank in your attack narrative.

5. Since `meterpeter` is a `PowerShell` program, you run it in `PowerShell`. Fortunately, `PowerShell` is now a multiplatform tool. You can find `meterpeter.ps1` in `git/meterpeter/meterpeter.ps1` on `kali`. To run it (if you are in that directory) execute `pwsh meterpeter.ps1`. Start `meterpeter`, start it on your server. When it starts, it gives a prompt for

   Local Host:

   You should provide `kali`'s IP in response. It then prompts for

   Local Port:

   You should provide whatever available local port you'd like to use for communication with the target. (Preferably a port numbered higher than 1,024 because low-numbered ports are reserved for use by root on Linux.) After that, you can just respond to queries with the `[Enter]` key. Eventually, it will tell you it is listening for connections. By default, `meterpeter` will generate file `Update-KB5005101.ps1` in the directory where you ran `meterpeter.ps1`. This is the `meterpeter` client corresponding to this server. You need to deliver it to your target host.

6. Once the `meterpeter` client runs, a connection will be established. When you get the `meterpeter>` prompt, you can run any `PowerShell`

command, or any command in the list of commands provided. You can navigate through the file system by executing `cd` commands. You can view directories by executing `ls` commands. (Yes, these are `PowerShell` commands.)

7. Write a partial PenTest report telling Hank how the `Veil` payload fared with AMSI and how well the `meterpeter` tool functioned. Provide evidence of your success with (at least partial) contents of the file you exfiltrated.