PenTest Lab Exercise Ex090 – PowerUp

Goal

Use PowerUp to identify possible misconfigurations on the costumes host in the artstailor.com network (then exploit any misconfigurations you might find).

Tasks

1. Log in to Netlab and schedule an Ex090 lab.
2. You will use rdesktop to share a directory, so make a subdirectory in /tmp for that purpose. Copy the PowerSploit PowerUp.ps1 module to that directory. (This PowerShell module should be in /usr/share/windows-resources/powersploit/PrivEsc on kali.)
3. Using rdesktop, connect to costumes.artstailor.com as some user whose credentials you have found. (Make sure you share that subdirectory of /tmp so that PowerUp.ps1 will be available to you.) What evidence do you have that you are correctly logged into the right host, that is, costumes.artstailor.com?
4. Once on the machine as the appropriate user, you can mount the shared directory using net use in a cmd shell, or just use (or cd to) the share name directly when you run PowerShell (with ExecutionPolicy set to bypass) to import the PowerUp.ps1 module. (Use Import-Module with the full path to the .ps1 file. Powershell will *not* look for modules in the current directory by default).
5. What happens when you try to import the PowerUp module? You can avoid this fate by using an obfuscated version of PowerUp, namely, /home/kali/Powershell/PowerDown.ps1 instead. Here are the changes that were made:
   - A number of comments that were or might have been used as signatures have been modified or deleted.
   - Function New-InMemoryModule was renamed Do-InMemoryModule.

- A string used as a signature was modified: 'System.AppDomain' was changed to 'System' + '.AppDomain'
- All functions named `Invoke-`*XXX* are renamed `Do-`*XXX*.
- Function `DownChar` was added. This decrements each character value in a string by one (i.e., to the previous character). Several Base64 strings recognized by Windows Anti-Malware Scan Interface (AMSI) were incremented by one character to avoid detection.

6. Once you have imported the module, you should execute the appropriate method in that module to check all the misconfigurations it can identify. (Consult your notes or harmj0y's `PowerUp` usage guide on the web to find out how to do this if you can't remember.)

7. When you identify a vulnerability, you may want to consult the Recipe For Root post concerning effective use of `PowerUp`. You may also want to consult the aforementioned `PowerUp` documentation on privilege escalation using the suggested `AbuseFunction`. Be careful, as some of the parameter names for the `AbuseFunction` may have changed since the Recipe For Root post was created. By the way, you **must** *never* use default or well-publicized credentials to provide access to a compromised system when engaging in a penetration test. To do so introduces more insecurity!

   Note: If you provide a password for a new account, default Windows security requires that it contain symbols from at least 3 of these character classes: *uppercase*, *lowercase*, *numbers*, *special*. If you don't provide a compliant password, the account *will not* be created.

8. If you have correctly employed the `AbuseFunction`, you will be able to create a local administrative user account. Get an Administrative shell using that account and use `mimikatz` to get the kind of information you can get. (It's in in `/usr/share/windows-resources/mimikatz/x64` on `Kali`). You should be particularly interested in information about users–even local user account passwords can be useful as people *often* reuse passwords. As a local admin, you also have the ability to look at lots of files on that host. If you find useful information make sure to store it on plunder.pr0b3.com for future reference.

   Of course, you realize that mimikatz.exe will be identified and quarantined by Windows 10's antivirus protection. You can turn AV protection off by selecting *Settings* from the command search and then

choosing *Update & Security* → *Windows Security* → *Virus & threat protection* → *Manage settings*. From there, you need to turn off *Real-time protection*. You can turn off *Cloud-delivered protection*, *Automatic sample submission*, and *Tamper protection* as well.

9. Prepare a partial penetration test report describing all your activities and the findings you have made. Provide a TTP for each distinct tactic you employed. Provide Findings with CVSS scores for each vulnerability you identified. Make sure you explain the appropriate remediation method and best practices for avoiding problems in the future.