PenTest Lab Exercise Ex060 – `VulnScan`

Goal

Run a `Nessus` vulnerability scan. Use `Metasploit` to gain shell access to a machine.

Tasks

1. Log in to the Netlab server, schedule the PenTest Ex060 Lab, start up the lab, and login to your Kali VM.

2. Start `Nessus` and then log in to its web interface. Create a new scan using the *Advanced Scan* template. Give the scan whatever name and description you desire. You will be scanning `ns.artstailor.com`, so provide its IP address as the Target.

3. Select the *Plugins* tab and **disable** all plugins. Then consult the OS type and list of services you got from your `nmap` scan from the previous exercise. You should **enable** every *Plugin Family* that might be appropriate for a scan of that host. For example, you would not enable *AIX Local Security Checks* because the host is not running IBM's AIX operating system, but you would enable *DNS* because the host provides name service. Be sure to include every service family that is applicable and all generic Plugin Families as well (such as *Backdoors*).

4. Click on the *Settings* tab to get back to the overall scan settings, then click on the *Assessment* setting entry.

    - In the *General* category, check the *Override normal accuracy* box and click *Show potential false alarms*. Also check *Perform thorough tests (may disrupt your network or impact scan speed)*.
    - In the *Brute Force* subcategory, unclick the *Only use credentials provided by User* setting.

5. Save your scan and then click the play button (near the right of the line on which the scan name appears in the *My Scans* list) to start the scan running. It may take a while, but if you selected the right collection of Plugin Families, it won't take *too* long.

6. Inspect the list of vulnerabilities identified. In particular, look at the high severity vulnerability that mentions `vsftpd`. Make note of the Metasploit module associated with this vulnerability.

7. Do what is necessary to start up the `Metasploit` console.

8. Once in `Metasploit`, search for the exploit mentioned by `Nessus` for the vulnerable service identified above and *use* that exploit. Then search for an appropriate payload. Set the options properly. (Look at the options carefully so you can be sure you've configured this to work with the service on the target machine.) Then run the exploit.

9. You may want to try using the `Metasploit` module `post/multi/manage/shell_to_meterpreter` to upgrade your connection to a `Meterpreter`. This could make file upload/download easier. If you do this, be careful to set the options correctly and check the sessions that are available after the post module completes its work.

10. Start `Wireshark` so you can inspect the packets that are sent back and forth between the attack and target host during the exploit. If you right-click on a single packet in the Packet List View of `Wireshark`, you can select `Follow TCP Stream` to see the input/output associated with that stream. Run the exploit several times and look at the interaction between the two hosts to determine what kind of username and password are being sent to `vsftpd` in order to open this backdoor communication. Use this together with information provided about the exploit to explain in your report how this exploit achieves access to the host. Several different ports are involved.

11. If you have a thorough understanding of this vulnerability, you may have noticed that you do not have the level of access you might expect. Feel free to include information about this in your report.

12. Write a report with a finding detailing the vulnerability you exploited. This will include any associated Mitre TTPs and CVSS severity scores. Also provide as simple a confirmation method as you can. Make sure to discuss how this vulnerability can be avoided or mitigated. Also, make sure to provide evidence that you were actually able to exploit the vulnerability successfully and access the system as a user. (Evidence of exploitation is often demonstrated by providing appropriately anonymized contents from exfiltrated files.)

13. A key is available in the file system on host `ns.artstailor.com`.