Content

Ex060.pdf 1 / 3 100%

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