Anthony Fecondo

MIS5211.001

Network Scanning Assignment

Nessus is a “proprietary comprehensive vulnerability scanner” developed by Tenable Network Security.[[1]](#endnote-1) The home version of Nessus can perform Badlock Detection, Bash Shellshock Detection, Credentialed Patch Audit, DROWN Detection, Host Discovery, Malware, and Basic Network scans. If you purchase Nessus you gain access to a variety of other scans in addition to those included with the Home package. Every scan you run displays any detected vulnerabilities (and assigns them a threat category ranging from informational to critical), an explanation of the test, recommended solutions, resources to learn more about the vulnerability, and the output of the specific test that Nessus ran.

When I used Nessus, I ran a variety of scans against my desktop computer that I use on a daily base. The scans I ran were Basic, Host Discovery, Web Application, Drown Detection, Bash Shellshock, and a Badlock scan. The host discovery was the simplest of these scans as it only ran an ARP who-is query (See Figure 1) to see if the host was up (which it was). The Badlock, Bash Shellshock, and Drown Detection scans all returned the same results, a single info level threat. After running the Nessus SYN scanner, a SYN ‘half-open’ port scanner that scanned for open ports and identified any that were open, the host, and the service using the port (See Figure 2), I was alerted of several open ports on my computer. Contrary to the small amount of information provided by the earlier tests, the Web Application and Basic scans revealed a significant amount of information (See Figures 3 and 4). As you can see in the figures, each of these scans returned a number of information level threats which I looked at and considered, but wasn’t too worried about. However, these scans also detected low and medium level threats. Naturally, as these warnings came up on my everyday use computer, I was a little alarmed. I read the information provided by Nessus and took the prescribed steps to rectify these exposures.

After experimenting with Nessus and analyzing the results the software provided I made note of the amount of information that can be gathered about a system by running these scans. The scan results listed information about the status of my system, the ports in use, the router I use, my operating system, the type and version of my HTTP server, my DNS server information, and more. In fact, Nessus was able to identify the majority of the information we went over in the reconnaissance unit of this class. In addition to the basic information of my system, Nessus also identified several higher priority threats such as potential XSS vulnerabilities or Clickjacking vulnerabilities. Nessus is great for evaluating and hardening the security of your personal system as it identifies potential vulnerabilities and provides suggestions as well as additional research on solving the problems, but it could also be a powerful weapon in the hands of hacker. A hacker could easily use Nessus to gather all the information he or she needs in order to plan and launch an attack.



Figure 1



Figure 2



Figure 3

Figure 4

1. https://en.wikipedia.org/wiki/Nessus\_(software) [↑](#endnote-ref-1)