Nessus LAN Vulnerability Scan

Project:

I performed a vulnerability scan of a LAN using Nessus. First, I identified all the hosts on the network, then I analyzed the most consequential vulnerabilities found for a single host (which was the router). Lastly, I remediated one of the more significant vulnerabilities.

Identify All Hosts on the LAN:

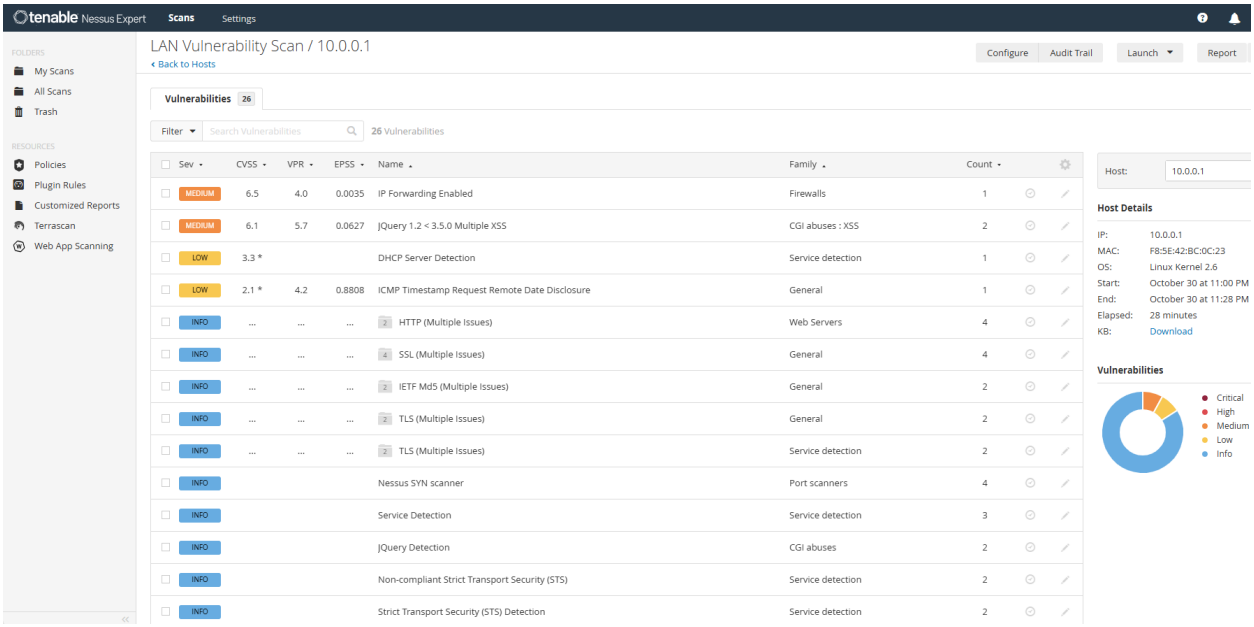
I identified 14 hosts on the LAN, with a total of 48 vulnerabilities detailed in Figure 1.

Figure 1: All LAN Hosts Identified by the Nessus

Investigate the Most Significant Vulnerabilities for Host 10.0.0.1 (The Router):

Listed below in Figure 2 are the vulnerabilities identified by Nessus for host 10.0.0.1 (the router).

Figure 2: Vulnerabilities for Host 10.0.0.1



The most significant vulnerability detected in the router was CVE-1999-0511, with a CVSS rating of 6.5. However, this vulnerability describes a remote host (other than a router or firewall) having IP forwarding enabled. Since the device in question is a router, the vulnerability can be categorized as a false positive.

The next most serious vulnerability identified in the router was CVE-2020-11023, with a CVSS rating of 6.1. CVE-2020-11023 is a JQuery-related vulnerability that allows for multiple types of XSS attacks. While a patch is available that would eliminate this vulnerability, it has not been incorporated by the ISP; and I do not have access to the firmware to update the device myself. Since the router in question was rented from an ISP, and a software update was not offered for the product, my choices were to accept the risk or purchase a new router; I chose to buy a new router. After its installation, I performed another vulnerability scan to see if the JQuery-related vulnerability was still present on the new device.

Since this is a new router, the internal IP address scheme of the LAN has changed, and that is reflected in the most recent vulnerability scan. To that point, the new router is identified as 192.168.68.1, shown in Figure 3. Finally, as you can see in Figure 3, this device does not have the JQuery-related vulnerability present, therefore CVE-2020-11023 has been effectively remediated.

Figure 3: Nessus Scan of New Router (192.168.68.1)