Marcus Wilson

MIS5211.001

October 26th, 2016

**Nessus Scan Analysis**

The scan that I performed revealed 19 total vulnerabilities and took about three minutes to run. One of these vulnerabilities was rated as Medium and 18 were rated as information only. A majority of the information alerts were basic networking details being displayed to the network on request. The focus of my analysis was on the only Medium alert. The Medium alert was in regards to SMB signing being disabled. The concern with this vulnerability is an unauthenticated attacker can exploit this to conduct man-in-the middle attacks against the SMB server.

The Server Message Block (SMB) operates as an application-layer network protocol that is used to provide shared access to files and printers across a local network. This is a protocol that is used heavily across Microsoft Windows computers. My Mac laptop had this capability turned on as I have my computers connected to share files across my home network.

Nessus had the following recommendation to eliminate the vulnerability:

“Enforce message signing in the host’s configuration. On Windows, this is found in the policy setting ‘Microsoft network server: Digitally sign communications (always)’. On Samba, the setting is called ‘server signing’. See the ‘see also’ links for further details.”

Since the recommendation was based on SMB running on a Windows OS, it took me a while to track down the root cause on my MacBook Air. After doing some research and seeing the relationship to file sharing I did some digging around my sharing settings. I turned off file sharing and re-ran the Nessus scan and it eliminated the SMB vulnerability and more than half of the info vulnerabilities that I was experiencing.

I decided to scan a few additional devices such as my Apple TV, PlayStation 4, and Xbox 360. I received all information only alerts and no concerning vulnerabilities. My next analysis would be on IoT devices since there is a growing concern around these devices and their growing volume on networks.

Scan Details

Source System: Windows PC Desktop

Source OS: Windows 7 Service Pack 1

Target System: MacBook Air

Target OS: Mac OS X 10.10

|  |  |
| --- | --- |
| 12053- Host Fully Qulaified Doman Name (FQDN) Resolution | 11219- Nessus SYN Scanner |
| 25220- TCP/IP Timestamps Supported | 43829- Kerberos Information Disclosure |
| 35716- Ethernet Card Manufacturer Detection | 10884- Network Time Protocol Server Detection |
| 11936- OS Identification | 10150- Windows NetBIOS SMB Info Disclosure |
| 54615- Device Type | 57608- SMB Signing Disabled |
| 45590- Common Platform Enumeration (CPE) | 11011- Microsoft Windows SMB Detection |
| 19506- Nessus Scan Information | 11219- Nessus SYN Scanner |
| 10287- Traceroute Information | 1066- Apple Filing Protocol Server Detection |
| 66717- mDNS Detection (Local Network) | 10785- Microsoft Windows NativeLanManager Discls. |