Shain Amzovski

MIS5211.001 – Introduction to Ethical Hacking

Analysis Report 2 – Scanning Exercise

Scan Results for a Windows Server 2008 R2

What is Nessus?

For this analysis report, I utilized Nessus to scan for vulnerabilities on an application server. Nessus is a remote security scanning tool that is made by Tenable. This tool scans computers or internet connected devices and raises an alert if it discovers any vulnerabilities. These vulnerabilities that raise alerts are generally used by malicious hackers to gain access to any computer you have connected to the network. Nessus is not a complete security solution, and should be used as only one small part of a good security strategy, as it does not actively prevent attacks.

Nessus Scan Results

I performed a Basic Network Scan on a Windows 2008 R2 Server with Service-Pack 1 installed. This server is a virtual server used for hosting an application that supports lecture capture. Since most of our servers have been migrated to Windows Server 2012 R2, I believed one of our older servers would come up with more vulnerabilities. In total, the results included 47 vulnerabilities. Of these vulnerabilities, 6 were considered Medium level, 4 were considered Low level, and 37 were considered Info. The 10 vulnerabilities that were considered either medium or low threat level, all had a common theme. The six medium threat level vulnerabilities were all related to SSL, and the four low risk vulnerabilities had to do with SSH. The three vulnerabilities I decided to investigate further was "SSL Certificate Cannot Be Trusted," "SSL Self-Signed Certificate," and "SSL RC4 Cipher Suites Supported (Bar Mitzvah)."

Recommended Solutions

To address the first and second vulnerabilities discussed in the Nessus Scan results, "SSL Certificate Cannot Be Trusted," and "SSL Self-Signed Certificate," the recommended solution by Nessus was to purchase or generate a proper certificate for this service. The "proper" way of addressing this issue would be to purchase a new SSL certificate from a Certificate Authority. Without spending money, a fix for this vulnerability would be to add the CA that signed the SSL certificate of the server in the list of "trusted CAs" of each of the clients that will access the server. The recommended solution for the third vulnerability "SSL RC4 Cipher Suites Supported (Bar Mitzvah)" is to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Nessus recommends using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Further Information About "Bar Mitzvah"

RC4 was originally a proprietary stream cipher, however, when the details of the cipher were leaked in 1994, the cipher has been publically studied and analyzed ever since. RC4 allows for variable key-length sizes between 40 and 256 bits. RC4 consists of two algorithms; Key scheduling algorithm (KSA), and a pseudo-random generation algorithm (PGRA). RC4 has several cryptographic weaknesses, mainly there are various biases in the RC4 keystream. Large, single-byte biases are prominent in the early positions of the RC4 keystream. These biases could be exploited by a broadcast attack, where the same plaintext is repeatedly encrypted under different keys. There are also double-byte biases in RC4. These biases were confirmed computationally and exploited when they were able to recover HTTP secure cookies. The Bar Mitzvah attack exploits the weak keys used by RC4 and allows an attacker to recover plain text from the encrypted information. This vulnerability allows for account credentials, credit card data, or other sensitive information to be potentially compromised.

Vulnerability	Risk	CVE Reference	Risk Rating	Recommendations
SSL Certificate Cannot Be Trusted	The server's X.509 certificate does not have a signature from a known public certificate authority.		Medium (6.4)	Purchase or generate a proper certificate for this service.
SSL Self-Signed Certificate	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.		Medium (6.4)	
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.	CVE-2013-2566 CVE-2015-2808	Low (2.6)	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.