Loi Tran
MIS5211.001

Nessus Scan Assignment

Nessus is a vulnerability scanning tool that allows penetration tester to scan a network to identify vulnerabilities that could be exploited by a malicious actor. Nessus GUI will provide the threat levels for services or vulnerabilities that it detects in five categories: Critical, High, Medium, Low, and Informational, with critical having the highest adverse impact on the system. It also provides description of the vulnerability, risk factors, and the Common Vulnerabilities and Exposures (CVE) number that could be used to help solve the problem.

My Nessus scan consisted of three different virtual machines (VM) that was created on a virtual network: one running a Windows 10 operating system (OS), and two running LinuxOS (Mesploitable and a Kali machine). According to the results of the scan, both the Windows 10 and the Kali VMs only had informational threat levels. The Mesploitable VM had all five threat levels including five critical vulnerabilities. This report will focus on the Metasploitable VM critical vulnerabilities and how it could be corrected. An important note to keep in mind about the "critical" threat level is that it does not consider mitigating controls that are in place.

Debian OpenSSH/OpenSSL – a bug existed in the random number generator that makes the confidentiality of a private key questionable. An attacker can obtain the private key and use it in a man-in-the-middle attack for a remote session. Corrective action: Update OpenSSL on the VM.

Rogue Shell Backdoor Detection – Research indicates that a backdoor has been created on the OS to allow attackers to access the computer without the need to authenticate. Corrective action: filter out remote connections to the port or alter the source to require authentication.

Unsupported Unix Operating System – This indicates that the operating system currently installed in the VM is no longer supported. This implies the VM have not been updated with new security patches and will have security vulnerabilities. Corrective action: check applications requirements that are running on the VM and see if it will be compatible with the updated/supported version of the OS. Update the OS if compatibility exists.

VNC Server 'password' Password – The default password for the VNC sever is "password" and easily exploitable by attackers. Corrective action: create a strong password.

Nessus is a great tool that will enable an organization to scan their networks for vulnerabilities. Although it is not a comprehensive tool, only scanning for common vulnerabilities as a free version, a paid version will offer more functionality and scanning capabilities. The level of details and corrective steps provided on the reports will help the organization make their systems more secure.

An organization could use Nessus to take an initial assessment of their security posture and immediately correct the problems that exists in their systems. By doing so, hiring an external penetration tester would yield more benefits, as they will be tasked to do more sophisticated scanning and vulnerability testing.