Introduction to Vulnerability Management - Course Challenge Report Template

Name of Individual Conducting Scanning:	Daniel Davidson
Nessus Scanner IP (IP of Kali VM):	10.0.2.15
Date & Time Scan Started:	10/21/21 at 11:46 PM CST
Date & Time Scan Finished:	10/21/21 at 11:26 PM CST
Security Issues Identified:	119

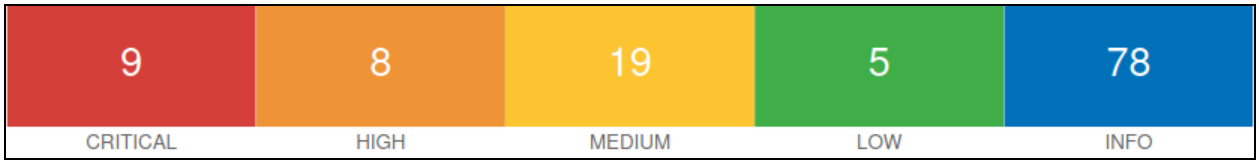
Instructions

1. Please refer to the Course Challenge Brief for instructions on what you are being asked to do.
2. Answer all questions mentioned below.

Overview

>> Provide an overview of the results from the scan. How vulnerable is this system?<<

Host: Metasploitable IP: 10.0.2.6



Assessed Threat Level: **High**

Overall, this system is very vulnerable. At the time of this writing it contains 119 total vulnerabilities with 19 rated **Medium**, 8 rated **High**, and 9 rated **Critical**. The system contains vulnerabilities such as backdoors, weak passwords, decipherable cryptographic keys that can be used to execute remote sessions, and the ability for eavesdropping data communications on the host which could allow it to serve as an initial foothold and potentially comprise other targets on the same network.

Download the following report to see a full list of vulnerabilities. Password: **sbt.nessusreports**

M2-sbt-report.csv M2-sbt-report.html M2-sbt-report.pdf

Top 5 Most Serious Security Issues (In priority order - most important first):

>> What are the 5 most critical issues with the scanned system? Talk about each one, and what could happen if an attacker exploits the vulnerability <<

The following vulnerabilities are ranked by Tenable's patented **Vulnerability Priority Rating (VPR)** system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.

1. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
   The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man-in-the-middle attack.

2. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**
   The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man-in-the-middle attack.

3. **UnrealIRCd Backdoor Detection**
   The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

4. **Samba Badlock Vulnerability**
   The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

5. **SMTP Service STARTTLS Plaintext Command Injection**
   The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase. Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

Top 5 - Remediations (In priority order - most important first):
>> What are the suggested remediation actions to address the top 5 most critical security flaws? Re-word them, don't just copy and paste Nessus' suggestions <<

1. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
   Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key material should be re-generated.

2. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**
   Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key material should be re-generated.

3. **UnrealIRCd Backdoor Detection**
   Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

4. **Samba Badlock Vulnerability**
   Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

5. **SMTP Service STARTTLS Plaintext Command Injection**
   Contact the vendor to see if an update is available.