## Lab #5: Assessment Worksheet

**How to Identify Risks, Threats & Vulnerabilities in an IT Infrastructure Using ZeNmap GUI (Nmap) & Nessus® Reports**

**Course Name: IAA202**

**Student Name: Phan Tuấn Minh**

**Lab Due Date: 7/10/2021**

**Overview**

One of the most important first steps to risk management and implementing a security strategy is to identify all resources and hosts within the IT infrastructure. Once you identify the workstations and servers, you now must then find the threats and vulnerabilities found on these workstations and servers.

Servers that support mission critical applications require security operations and management procedures to ensure C-I-A throughout. Servers that house customer privacy data or intellectual property require additional security controls to ensure the C-I-A of that data. This lab requires the students to identify threats and vulnerabilities found within the Workstation, LAN, and Systems/Applications Domains.

**1. What are the differences between ZeNmap GUI (Nmap) and Nessus?**

Instead of using Nessus to look for specific vulnerabilities against a known quantity of hosts, NMAP discovers active IP hosts using a combination of probes. On the other hand, Nessus takes the open ports into account and notifies you if these ports have potential security vulnerabilities attached to them. Nessus is typically installed on a server and runs as a web-based application. Nessus uses plugins to determine if vulnerability is present on a specified machine

**2. Which scanning application is better for performing a network discovery reconnaissance probing of an IP network infrastructure?**

In SSIDer is a Wi-Fi network scanner for the 32-bit and 64-bit versions of Windows XP, Vista, and 7. It is free and open source. The software uses the current wireless card or a wireless USB adapter and supports most GPS devices (namely those that use NMEA 2.3 or higher). Its graphical user interface shows MAC address, SSID, signal strength, hardware brand, security, and network type of nearby Wi-Fi networks. It can also track the strength of the signals and show them in a time graph.

**3. Which scanning application is better for performing a software vulnerability assessment with suggested remediation steps?**

The annual SANS Top 20 classifies most of these dangerous holes for both Windows and Unix, and prescribes best practices for patching and remediation. Also, the SANS Top 20 arranges vulnerabilities into 10 classes for each platform with categories of vulnerabilities within them.

**4. How many total scripts (i.e., test scans) does the Intense Scan using ZenMap GUI perform?**

The Intense Scan can take 3 to 5 minutes to complete all 36 test scripts. When the scan has finished, Zenmap will display the Nmap done command.

**5. From the ZenMap GUI pdf report in classroom, what ports and services are enabled on the device?**

**PORT SERVICE VERSION**

**21/tcp ftp vsftpd 2.3.4**

**22/tcp ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)**

**23/tcp telnet Linux telnetd**

**25/tcp smtp Postfix smtpd**

**53/tcp domain ISC BIND 9.4.2**

**80/tcp http Apache httpd 2.2.8 ((Ubuntu) DAV/2)**

**111/tcp rpcbind 2 (RPC #100000)**

**139/tcp netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)**

**445/tcp netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)**

**512/tcp exec netkit-rsh rexecd**

**513/tcp login?**

**514/tcp shell?**

**1099/tcp java-rmi Java RMI Registry**

**1524/tcp shell Metasploitable root shell**

**2049/tcp nfs 2-4 (RPC #100003)**

**2121/tcp ftp ProFTPD 1.3.1**

**3306/tcp mysql MySQL 5.0.51a-3ubuntu5**

**5432/tcp postgresql PostgreSQL DB 8.3.0 - 8.3.7**

**5900/tcp vnc VNC (protocol 3.3)**

**6000/tcp X11 (access denied)**

**6667/tcp irc Unreal ircd**

**8009/tcp ajp13 Apache Jserv (Protocol v1.3)**

**8180/tcp http Apache Tomcat/Coyote JSP engine 1.1**

****

**6. What is the source IP address of the device (refer to the pdf report)?**

**172.30.0.30**