Lab # 5 — Assessment Worksheet

**Course Name and Number: IAA202**

**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Mai Hoang Dinh**

## **Identify Threats and Vulnerabilities in an IT Infrastructure**

***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.

***Lab Assessment Questions & Answers***

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

NMAP is primarily a host detection and port discovery tool. 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 handNessus takes the open ports into account and notifies you if these ports have potential security vulnerabilities attached to them. Nessus is typically installed on aserver and runs as a web-based application. Nessus uses plugins to determine if vulnerability is present on a specified machine.

1. **Which scanning application is better for performing a network discoveryreconnaissance probing of an IP network infrastructure?**

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

1. **Which scanning application is better for performing a softwarevulnerability assessment with suggested remediation steps?**

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

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

Loaded 36 scripts for scanning.

1. **From the ZenMap GUI pdf report page 6, what ports and services areenabled on the Cisco Security Appliance device?**

22/tcp open ssh Cisco SSH 1.25 (protocol 2.0).

1. **What is the source IP address of the Cisco Security Appliance device(refer to page 6 of the pdf report)?**

172.30.0.1

1. **How many IP hosts were identified in the Nessus® vulnerability scan? List them.**

9 IP addresses (5 hosts up) scanned in 49.39 seconds, 256 IP addresses (5hosts up) scanned in 5433.44 seconds.

1. **While Nessus provides suggestions for remediation steps, what else does Nessus provide that can help you assess the risk impact of the identified software vulnerability?**

Control System Intelligence - In addition to its low impact vulnerabilityscanning features, Nessus contains specific control system intelligence in the formof Bandolier security audit files for control system applications and the SCADAPlugins family.

1. **Are open ports necessarily a risk? Why or why not?**

An open port is not necessarily dangerous! - You are only at risk if the program using the port contains harmful code. So there is no reason to close all ports in your system. In fact without your ports being open, the Internet simplywouldn't work!

1. **When you identify a known software vulnerability, where can you go toassess the risk impact of the software vulnerability?**

Go to Servers > Software Risks or click the Software icon (.)

1. **If Nessus provides a pointer in the vulnerability assessment scan report tolook up CVE-2009-3555 when using the CVE search listing, specify what this CVE is, what the potential exploits are, and assess the severity of the vulnerability.**

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to makeit easier to share data across separate vulnerability capabilities (tools, repositories,and services) with this "common enumeration." CVE only contains the standardidentifier number with status indicator, a brief description, and references to relatedvulnerability reports and advisories. A CVE Identifier will give you a standardizedidentifier for any given vulnerability or exposure. By knowing this, the identifier will allow you to quickly and accurately access information about the problemacross multiple information sources that are.

1. **Explain how the CVE search listing can be a tool for security practitionersand a tool for hackers.**

The CVE search listing can be a tool for security practitioners byshowing possible vurnerabilities in their systems as well as way to fix it.Hackers could use the CVE to avoid programs they can and cannot use tohack the system of their choice.

1. **What must an IT organization do to ensure that software updates and security patches are implemented timely?**

An IT organization should be checking regularly from the vendor for patches tothe software to ensure that security fixes and software versions are up to date and running newest product details, and by setting up a time for updates whencomputers and servers are not in use.

1. **What would you define in a vulnerability management policy for anorganization?**

Define the level of security that an organization wants to maintain.Set guidelines for vulnerability management practices. Classify vulnerabilities by risk/threat and remediation effort. Determine how often scans will be performed. Define access control policy for all devicesconnected to the network. Outline the consequences of compliance.

1. **Which tool should be used first if performing an ethical hacking penetration test and why?**

Wireshark should be used because it just scans the network for open ports and IP’s but many tools can be used just to scan the network, as long as this tool is not trying to penetrate the security of the network or gainaccess to files.