ACIT 4630 – Lab 2 – Vulnerability Scanning

Notes:

If you worked with a partner in Lab 1, you will be working with the same partner for this lab.

Instructions:

We are going to use the Kali VM and the Metaploitable2 VM we created in the previous lab.

An attacker or a pen tester goes through the reconnaissance phase first to look at the overall environment, identify specific targets, and focus on target enumeration.

Host discovery and scanning using nmap

- (Q1) What is the purpose of the -sn option in nmap?
- (Q2) In the previous lab, you used nmap to find what services are running on what ports in the Metasploitable2 VM. Which nmap option gives you the version of those services? why is it important for vulnerability scanning?
- (Q3) Try scanning Metasploitable2 VM from your Kali machine using -A option with nmap. What additional information about the open ports on Metasploitable2 VM can you get by using this option?
  - Watch this video for more info

Exploring Vulnerabilities

After we complete enumerating (retrieving and collecting services, usernames, computers, ... on a network) Metasploitable 2, we need to look for known vulnerabilities for operating systems and services running on this machine. Do the following steps for **ftp (on port 21)** and **irc** services running on Metasploitable 2:

- From your previous nmap results, find the software and the version for the service and Google this info to see if this specific version of the software has any known vulnerabilities.
- Nmap has a comprehensive library of scripts that provide many advanced capabilities. Find and use nmap with a script that scans a target for a vulnerable version of these softwares.
  - Hint: use --script option
  - Hint: You should provide the port the service is running on
- (Q4) What vulnerabilities did you find – both from Google and using the script?

Vulnerability Scanning Report

Many tools can be used for vulnerability scanning. It's important to properly analyze the scan report and come up with how to remediate existing vulnerabilities. Please download the Metasploitable vulnerability scan called *report-cbf742b1-e4ad-4cda-814b-d26c2c830733.pdf* (generated by OpenVAS scanner).

- (Q5) Some of the information on a vulnerability scan report might be incorrect. What kind of potential **errors** should you be looking for on such a scan report?
- (Q6) Look at how found vulnerabilities were scored high, medium, and low using their CVSS score. Watch this video and list different parts of the CVSS Base Vector.
- (Q7) List different solution **types** suggested in the report for found vulnerabilities.
- (Q8) Watch this video and list the factors to consider when prioritizing found vulnerabilities for remediation.

Submission For Lab 2:

- Create a report answering the seven questions in the lab above.
- Walk through your report with your instructor.
- Submit your report to the Learning Hub in PDF format.

This lab is due at the beginning of the Week 3 class and is worth a maximum of 10 marks.