

## ISEC 2076 Assignment 2 – Vulnerability Analysis

**Issued Date: September 18, 2024**

**Due Date: October 9, 2024**

### Preamble

When tasked with evaluating a security profile for an organization, one important step is to understand the “Attack Surface” that exists with respect to the endpoint devices. In this case, we will limit the endpoint devices to the computers in the D317 lab and we will begin with that aspect of the attack surface that deals with their network interfaces as well as probing the installed software and operating system of each endpoint and the associated vulnerabilities

### Requirements

#### **Part 1**

1. Download and install a copy of Nessus essentials on either the lab machine to which you have admin access or a bridged VM.
2. Gather the IP address (172) of your machine and the one next to you at the pod.. Make sure you have the person next to you verify the IP addresses and you should do the same for them.
3. Update the vulnerability plugins for Nessus.
4. Conduct an unauthenticated scan (all ports) against your own IP and the one next to you at your pod. Save your scan results to an HTML file and submit that file along with your report to the dropbox.
5. Obtain an administrator account username and password for your machine and the one next to you at the pod.
6. To prepare for the authenticated scan, enable Remote Registry on your machine, set domain to “.”, make sure you enable remote registry access in your Nessus profile. Each IP that is scanned must have Remote Registry enabled have
6. ONCE THE ADMIN ACCOUNT HAS BEEN SET UP ON THE TWO MACHINES, conduct a authenticated scan against the IPs using the Administrative User Account and Password assigned above. Save your scan results to an HTML file and submit that file along with your report to the dropbox.

#### **Part 2**

1. Build a report that shows the results from the unauthenticated scan. The report should list any reported vulnerabilities. Vulnerabilities should be identified and accompanied by a brief description of the vulnerability **in your own words**. This report should be targeted at management. Therefore, it should not just be the output from Nessus.
2. Build a report that shows the results from the authenticated scan. For each computer, list any Medium, High or Critical vulnerabilities discovered along with a brief, non-technical, description **in your own words** of each. REMEMBER TO CHECK YOUR OUTPUT TO SEE IF THERE IS MESSAGE TELLING YOU THAT LOGIN OR REMOTE REGISTRY WAS NOT AVAILABLE. IF SO, CORRECT YOUR LOGIN CREDENTIALS AND/OR START THE REMOTE REGISTRY SERVICE ON THAT TARGET COMPUTER AND RESCAN.

## ISEC 2076 Assignment 2 – Vulnerability Analysis

Issued Date: September 18, 2024

Due Date: October 9, 2024

### Submission Requirements

Your submission will include your main project document together with 2 scan files (HTML).

The assignment is to be uploaded to a Brightspace drop box on or before the due date. The document is to be of professional quality including content, layout, font, grammar, spelling, overall appearance, and structure. *Hint - You should envision that this is a report that you have been asked to formulate for a client or an employer.* Do your best work.

**NOTE: There is no requirement for APA referencing style in this document. For each vulnerability listed in your report, simply include the URL where you found a description.**

Document name (i.e., filename) **MUST** be of the format: **YourLastName-YourFirstNameISEC2076-As2**

Your document **MUST** include a separate title page containing the **course category** (ISEC) and **number** (2076), **your name**, the **assignment number** (2) and the **assignment title** ("Vulnerability Analysis"). All answers to the requirements above should be clearly labelled, and answers clearly written.

### ***Note regarding individual work vs group work***

***Group work is encouraged for the purposes of gathering the IP addresses. Each student's is expected to find the remaining information on their own. Each scan and scan file will be the result of individual work. Each student must run their own scan and compile their own results.***

### Rubric

This assignment is worth 10% of your final mark and it is scored out of 40 points using the following rubric.

Please note that a pass is 60% (24 points) and if all categories are "Condition Somewhat Met" then you can only score a maximum of 20 points and will therefore not receive a passing grade.

Neatness counts!

Total marks:40

Rubric	Condition Not Met	Condition Somewhat Met	Condition Met
Document Names and Sections are clear and well formatted as required.	0	2	4
Each question and task is complete and correct	0	15	30
Assignment submission shows obvious v effort and care.	0	3	6
Total Maximum Points Available by Column	0	20	40