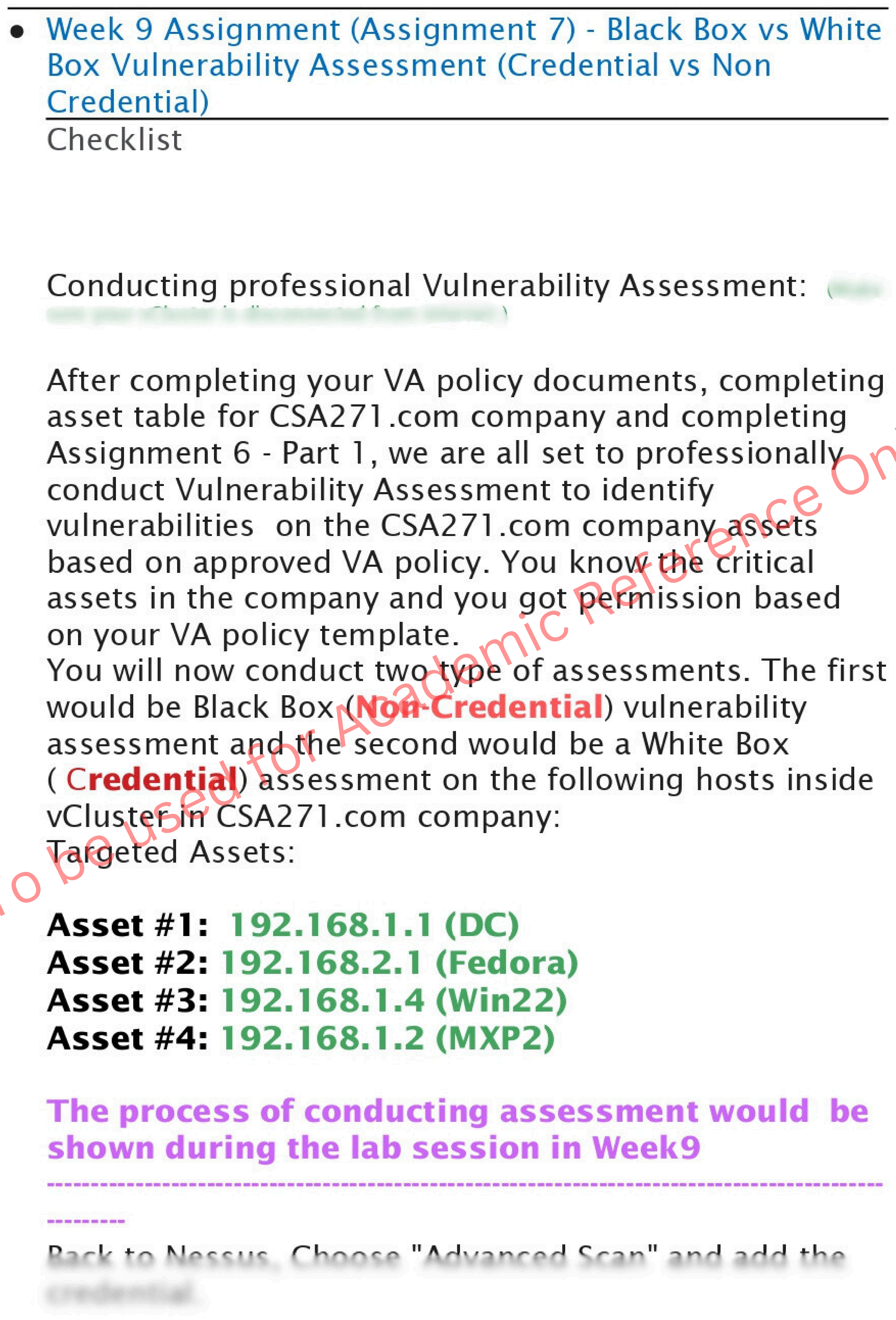
```
std::map<HWND, CddaDataModel*> WINDOW_TO_MODEL;
static char FirstDriveFromMask(ULONG unitmask) {
    char i;
    for (i = 0; i < 26; ++i) {
        if (unitmask & 0x1) {
            break;
        }
        unitmask = unitmask >> 1;
    }
    return(i + 'A');
}

LRESULT CALLBACK CddaDataModel::StaticWndP
    switch (uMsg) {
        case WM_DEVICECHANGE: {
            if (wParam == DBT_DEVIC
```

CSA271

PROGRAMMING IN C



- Week 9 Assignment (Assignment 7) - Black Box vs White Box Vulnerability Assessment (Credential vs Non Credential)

Checklist

Conducting professional Vulnerability Assessment: ([illegible])

After completing your VA policy documents, completing asset table for CSA271.com company and completing Assignment 6 - Part 1, we are all set to professionally conduct Vulnerability Assessment to identify vulnerabilities on the CSA271.com company assets based on approved VA policy. You know the critical assets in the company and you got permission based on your VA policy template.
You will now conduct two type of assessments. The first would be Black Box (**Non-Credential**) vulnerability assessment and the second would be a White Box (**Credential**) assessment on the following hosts inside vCluster in CSA271.com company:
Targeted Assets:

Asset #1: 192.168.1.1 (DC)
Asset #2: 192.168.2.1 (Fedora)
Asset #3: 192.168.1.4 (Win22)
Asset #4: 192.168.1.2 (MXP2)

The process of conducting assessment would be shown during the lab session in Week9

Back to Nessus, Choose "Advanced Scan" and add the credential

For Linux you choose SSH tab
For Windows Server you choose Windows tab to enter credentials:

and then save it.

Note: For credential scan on Linux machine (Fedora), make sure the ssh service is active & running using this command:

```
# service sshd status
```

You see this:

If it is not active, activate it (How you activate ssh service on Linux?

Launch the Scan

Now you are ready to launch scan from "My Scan" Tab and click on Play button. It takes a while, till Vulnerability Assessment get finished.
Like below:

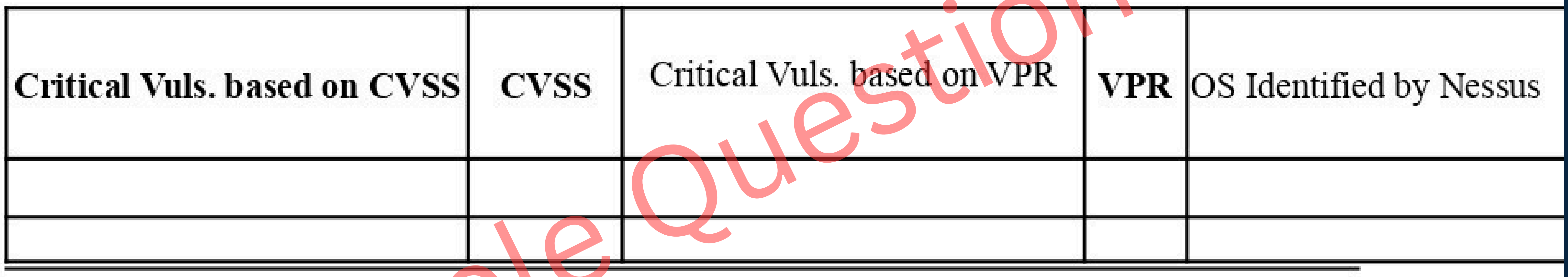
Take screenshot and add to your report.
You can now analyze each vulnerability one by one.

Q1: How many Critical and High vulnerability you have identified in the server?
STEP 2- At this stage we are ready to analyze the report based on Nessus finding.
Note that for each assessment, you will generate one report. (8 reports in total), Due to the fact that the new policy under ITS department, don't allow vCluster have access to internet all the time, you can take screenshots of the reports, as follow:

I have prepared a sample Nessus report for both BlackBox (Non credential) vs WhiteBox (Credential) scan on windows uploaded in Week9 course folder. You will do the same for each above host.
Here is the results of WhiteBox assessment on DC.
(Take screen shot)

Analyze the assessment results:

3- Add critical vulnerabilities to your asset table, under column name "**Critical Vulnerability Based on CVSS**" and add a short explanation for each critical vulnerability in the asset table under mentioned column. Next, add another column for score of vulnerability (Name: **CVSS**) which is identified by Nessus (you can find it in the report). Add the value of CVSS of each **critical** vulnerability to that column.
Add critical vulnerabilities to your asset table, under column name "**Critical Vulnerability Based on VPR**". Next to that column, add another column for score of vulnerability (Name: **VPR**) which is identified by Nessus (you can find it in the report). Add the value of VPR of each critical vulnerability to that column. (like below table)



Critical Vuls. based on CVSS	**CVSS**	Critical Vuls. based on VPR	**VPR**	OS Identified by Nessus

Add another column (Title column "**OS Identified by Nessus**". [fill this column with OS identified in Nessus scan results], alternately you can use **host discovery** policy (OS Discovery Option) to identify those OSes.
Q2- What host's OS, has been identified correctly by Nessus?
(Compare the results in Q1, with column regards to "**OS identified by Nmap**" previously added to your asset table)

Generate professional assessment report

Once you finished your scan which will take sometimes. You will need to save the results in a format of official report. Nessus create a professional report for you.

To do so click on your scan's Name, then on the top right of Nessus window, you will find the Report item, choose HTML report format from the drop-down list.

Remember, Nessus Essential has limit of 16 individual IPs to be scanned. But if you scan **same** host IP several times it doesn't count. So use it wisely

Deliverable:

Submit following components:

a) Answer to the Questions above

b) Generated reports (8 reports two for each host) by Nessus and save it for later. (No need to submit them yet)

c) Screenshots from STEP 2 above (with green font, two ScreenShots for each report)

d) Updated asset table on Excel sheet instead of Word file if you haven't done so)

Due date: written on the Dropbox

- Sample - Scan results of Server2019 - Credential Scan
  Web Page

- Sample - Scan results of Server2019 - Non Credential Scan
  Web Page

- Week 9 - Lecture Note - Professional Assessment CVSS/VPR
  PDF document

- Nessus -Essential