This exercise will introduce trainees to the advanced settings within the Nessus Vulnerability Scanner. Trainees will modify scan settings to perform different types of scans and to learn about the different functionalities Nessus provides. Trainees will then compare the results of a Nessus scan against the results of a NMAP scan against the same target and discuss the differences and similarities between the two tools. Lastly, trainees will use the "Export" feature to generate Nessus reports.

Equipment: Windows 7-2 VM

1. Nessus enables a reduction in attack surface by enforcing compliance and system hardening policies. Nessus users easily create and customize compliance and security policies while also being able to manage scan results, schedules, and policies. Nessus provides an automated process and provides more control over the update process. Nessus easily integrates into existing security processes with a new API, which is fully documented and accessible from within the Nessus UI.

2. Log into the Windows 7 virtual machine.

    a. Username: Administrator / Password: P@ssw0rd

3. Click the start button → All Programs → Tenable Network Security → Nessus → Nessus Web Client

    a. This will open a Chrome browser.
    b. Click "Advanced."
    c. Click "Proceed to localhost (unsafe)"

4. Log into Nessus.

    a. Username: admin / Password: admin

5. Click on Policies on the top bar and proceed to click on "New Policy"

6. Click on "Host Discovery".

7. Name your policy and define it, click Next.

8. Notice the different types of "Discovery type"

    a. How is this different/similar to NMAP? ______________________________

9. Choose "Host Enumeration". Click "Save".

10. Go back to the Policy page and click on New Policy again then proceed to Advanced Policy.

11. Click the "Preferences" link on the left and then choose "Service Detection" from the dropdown menu.

    a. Here you will find settings related to how Nessus does service discovery – specifically SSL.
    b. Notice the default is the search for SSL on "Known SSL ports".

        i. List one known SLL Port: ______________________________

        ii. Why would you want to search for SSL on "All Ports"?
        ____
        ____

12. Included in the "Preferences" section are a few other settings of interest: Antivirus Software Check, Do not scan fragile devices, Malicious Process Detection and SMTP Settings.

    a. Nessus is configured with a standard accuracy setting but you can change the setting to hide false alarms or show alarms for further analysis.
    b. The "Antivirus" setting allows the scanner to determine how long it has been since the last antivirus update.

        i. This is ideal in an organization that has antivirus policy/requirements established.

        ii. Why might you want to add application/file white/blacklisting to your scan?
        ____
        ____
        ____

    c. The "SMTP" setting will provide information about SMTP Headers for whichever domain is specified.

        i. Note: All of these additional scan features add extra time and potential strain on the network. Again, use with caution.

13. On the left side of the screen you will see a "Credentials" link – clicking this link will allow you to enter specific credentials for different services on the network.

        i. As discussed in the module – credential scanning potentially gives you more access to systems in order to perform a "deeper" scan.

14. The “Web Application Tests Settings” section under Preferences is where you can decide to include web application scanning if you have web servers/services running in the network you are scanning.

15. You can create a more advanced scan using a combination of the different options available in the Preferences section. Be sure to look at the different options when building your scans to highlight services you want to assess with your scan.

    a. Some of the options might help avoid detection (or at least attempt to).

        i. Scan IP addresses in random order, for example.
            1. Note: This is not available in this version of Nessus.
            2. Note: Nessus is a very “noisy” application and should not be considered when stealth is desired.

        ii. Nessus does have the capacity to cause a denial of service (DoS) event on the network you are scanning. Use caution when running Nessus – especially when modifying some of the more advanced scanning features –ie. those discussed in this lab.

16. Now that we have reviewed the advanced scanning features of Nessus it is time to finalize a scan.

    a. Feel free to create the scan as you see fit, but take into account the importance of systems availability to your organization.
    b. You will need to return to the “General Settings” area and select “Basic” from the dropdown menu and give your new advanced scan a name.
        i. Click “save” to save all the advanced options you selected.

17. Click “Scans” at the top of the page and fill in the information to begin a new scan.

    a. Be sure to enter a name for your scan: “Advanced Network Scan (Custom)
    b. Add a description: include information about the different advanced settings you picked.
    c. Make sure to select your new advanced policy.
    d. Enter the IPs for the target machines:
        i. 192.168.0.100
        ii. 192.168.0.20
        iii. 192.168.0.221
        iv. 192.168.0.125
        v. 192.168.0.50
        vi. 192.168.0.98

18. Click “Launch” and the scan will begin to run.

19. As the Nessus results begin to populate use the results to answer the following:

a. **Remember to click your scan results to view them.**

b. What type of operating system (OS) was identified at 192.168.0.100?

____

c. What type of operating system (OS) was identified at 192.168.0.20?

____

d. What type of operating system (OS) was identified at 192.168.0.221?

____

e. What type of operating system (OS) was identified at 192.168.0.125?

____

f. What type of operating system (OS) was identified at 192.168.0.50?

____

g. What type of operating system (OS) was identified at 192.168.0.98?

____

NOTE: BEFORE PROCEEDING TO THE NEXT STEP IT IS ADVISED YOU WAIT FOR THE NESSUS SCAN TO COMPLETE BEFORE EXECUTING A SIMULTANEOUS NMAP SCAN ON THE SAME HOST MACHINES. IF YOU DO NOT WAIT YOU WILL LIKELY CAUSE A DENIAL OF SERVICE SITUATION.

20. Minimize the Nessus scan and click the “NMAP – Zenmap GUI” icon on the desktop.

21. Enter the targets from the list above in the “Target” section with a space between each target.

22. Select “Intense Scan” from the “Profile” menu.

23. Click “Scan”

24. Wait for the NMAP scan to finish and compare results to the Nessus scan.

25. Use the results from the NMAP scan to help answer the questions in #21.

26. What are three things different or similar about Nessus and NMAP?

    ____

    ____

    ____

    ____

27. Provide an example where/why you would use one over the other, be specific. Is there an instance where you would not want to use either?

    ____

    ____

    ____

    ____

    ____

    ____

    ____

    ____

28. Return to the Nessus application – log in again if necessary.

    a. Username: admin / Password: admin

29. Assuming your scan has finished, click on the row that contains the most recent Advanced Network scan.

    a. At the top of the screen click on “Export”.

        i. These are the output file formats Nessus provides.

    b. Choose “HTML”.
    c. Drag the Hosts Summary (Executive) under Report Content and click “Export”.
    d. Open the file with the defaulted browser “click OK”.
    e. Review your results.

f. Go back to the “Export” feature and drag a different report format over to the Report Content section.
g. Click “Export” again.
h. Compare the results from the Executive scan to the Custom scan.

30. Nessus also allows for automated scanning via a schedule. Remember back to when we launched the scan there was an option to set reoccurring scans.

31. There is also the option to have the scan results emailed to a list of recipients.

32. You can also export the out as “Nessus” output which will allow you to share results between different Nessus clients.