

Lab #2 - Assessment Worksheet

Performing a Vulnerability Assessment

Course Name and Number:

Student Name:

Instructor Name:

Lab Due Date:

Lab Assessment Questions & Answers

1. What is Zenmap typically used for? How is it related to Nmap? Describe a scenario in which you would use this type of application.
2. Which application can be used to perform a vulnerability assessment scan in the reconnaissance phase of the ethical hacking process?
3. What must you obtain before you begin the ethical hacking process or penetration test on a live production network, even before performing the reconnaissance step?
4. What is a CVE listing? Who hosts and who sponsors the CVE database listing web site?
5. Can Zenmap detect which operating systems are present on IP servers and workstations? Which option includes that scan?
6. How can you limit the breadth and scope of a vulnerability scan?

7. Once a vulnerability has been identified by Nessus, where would you check for more information regarding the identified vulnerability, exploits, and any risk mitigation solution?
8. What is the major difference between Zenmap and Nessus?
9. Why do you need to run both tools like Zenmap and Nessus to complete the reconnaissance phase of the ethical hacking process?