# Identify threats and vulnerabilities in an it infrastructure

1. What are the differences between ZeNmap GUI (Nmap) and Nessus? NMAP is primarily a host detection and port discovery tool. Instead of using Nessus to look for specific vulnerabilities against a known quantity of hosts, NMAP discovers active IP hosts using a combination of probes. On the other hand Nessus takes the open ports into account and notifies you if these ports have potential security vulnerabilities attached to them. Nessus is typically installed on a server and runs as a web-based application. Nessus uses plugins to determine if a vulnerability is present on a specified machine.

2. Which scanning application is better for performing a network discovery reconnaissance probing of an IP network infrastructure? inSSIDer is a Wi-Fi network scanner for the 32-bit and 64-bit versions of Windows XP, Vista, and 7. It is free and open source. The software uses the current wireless card or a wireless USB adapter and supports most GPS devices (namely those that use NMEA 2. 3 or higher). Its graphical user interface shows MAC address, SSID, signal strength, hardware brand, security, and network type of nearby Wi-Fi networks. It can also track the strength of the signals and show them in a time graph.

3. Which scanning application is better for performing a software vulnerability assessment with suggested remediation steps? The annual SANS Top 20 classifies most of these dangerous holes for both Windows and Unix, and prescribes best practices for patching and remediation. Also, the SANS Top 20 arranges vulnerabilities into 10 classes for each platform with categories of vulnerabilities within them.

4. How many total scripts (i. e., test scans) does the Intense Scan using ZenMap GUI perform? The Intense Scan can take 3 to 5 minutes to complete all 36 test scripts. When the scan has finished, Zenmap will display the Nmap done command

5. From the ZenMap GUI pdf report page 6, what ports and services are enabled on the Cisco Security Appliance device? 22/tcp open ssh, 53/tcp open domain, 80/tcp open http

6. What is the source IP address of the Cisco Security Appliance device (refer to page 6 of the pdf report)? 192. 168. 0. 1

7. How many IP hosts were identified in the Nessus® vulnerability scan? List them.

8. While Nessus provides suggestions for remediation steps, what else does Nessus provide that can help you assess the risk impact of the identified software vulnerability? Through passive monitoring, PVS can reveal devices and software on the network that are not authorized, or that may indicate a network compromise.

9. Are open ports necessarily a risk? Why or why not? They are a risk because a trojan can be used to transmit data to an attacker. They hold a port open, e. g. Port 31337. The attacker connects to the trojan and sends requests to do a certain task, for example to make a screenshot. The trojan makes the screenshot and sends the image via the port to the attacker. On newer trojans, the port number is quite freely configurable, which makes identifying the trojan by the port number difficult. There are no control

mechanisms available which can prevent a trojan from using an specific port. If a trojan does use the port 80, for instance, a novice user could imagine the program is a webserver, and may even simply ignore the port.

10. When you identify a known software vulnerability, where can you go to assess the risk impact of the software vulnerability? Nessus can detect thousands of problems, and it classifies each as one of four different " risk severities": Critical, High, Medium, and Low. These severities are determined by the associated Common Vulnerability Scoring System (CVSS) score of the vulnerability. Nessus " risk severities" are based on CVSS, which is a classification system for the exploitability of software vulnerabilities and exposures. That is, it only provides information on how easily a vulnerability can be exploited by an attacker, given the opportunity, and what the vulnerability allows an attacker to do with the specific system.

11. If Nessus provides a pointer in the vulnerability assessment scan report to look up CVE-2009-3555 when using the CVE search listing, specify what this CVE is, what the potential exploits are, and assess the severity of the vulnerability. CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this " common enumeration." CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories. A CVE Identifier will give you a standardized identifier for any given vulnerability or exposure. Knowing this

identifier will allow you to quickly and accurately access information about the problem across multiple information sources that are CVE-compatible.

12. Explain how the CVE search listing can be a tool for security practitioners and a tool for hackers. They will know what programs they can use and what they can’t use to hack systems.

13. What must an IT organization do to ensure that software updates and security patches are implemented timely? Establishing a patch management plan. A process should be developed to evaluate the criticality and applicability to the software patch.

14. What would you define in a vulnerability management policy for an organization? A good Vulnerability Management Program gives an organization a great view of the effectiveness of the security controls they have implemented. Your policy should have clearly defined timelines for how long a system owner has to address a vulnerability on a system they own. As an example, your policy may require vulnerabilities which pose an extreme technical risk to be addressed within a five-day window, a vulnerability which poses a high technical risk be addressed in a two-week window, and a vulnerability which poses a medium technical risk be addressed within a month.

15. Which tool should be used first if performing an ethical hacking penetration test and why? Nmap, Nmap Security Scanner is an extremely powerful port scanner and auditing utility. It is an open source application and available at no cost. Nmap runs on many different operatingsystems,

including all NT-based versions of Windows, UNIX, Linux, Solaris, OpenBSD, Mac OS X, and Amiga. It is available in both 32-bit and 64-bit.