Take Test: Vulnerability scanning and Web security

Test Information

Description	
Instructions	
Timed Test	This test has a time limit of 40 minutes.This test will save and be submitted automatically when the time expires. Warnings appear when **half the time**, **5 minutes**, **1 minute**, and **30 seconds** remain.
Multiple Attempts	Not allowed. This Test can only be taken once.
Force Completion	Once started, this test must be completed in one sitting. Do not leave the test before clicking **Save and Submit**.
	Your answers are saved automatically.

QUESTION 1 **1 points** ✓ Saved

If a Nessus scan reports that a system is vulnerable to a remote exploit with arbitrary code execution, this means:

● An attacker MAY be able to run commands on this service
○ An attacker WILL be able to run commands on this service
○ An attacker WILL NOT be able to run commands on this service
○ An attacker WILL be able to get a shell

QUESTION 2 **1 points** ✓ Saved

Which of the following tools includes scripts for performing vulnerability analysis scans?

○ Msfconsole
○ Amap
● Nmap
○ Dig

QUESTION 3 **1 points** ✓ Saved

Which of the following is NOT an advantage of vulnerability scanning vs penetration testing

○ Less likely to cause accidental damage
● Thorough and complete
○ Automated and easy to conduct
○ Systematic and consistent results

QUESTION 4 **1 points** ✓ Saved

If Nessus detects that a server has port 443 open, this most likely means:

● That it is probably a web server
○ That the system is vulnerable to attack
○ That it is probably a web server, and WILL be vulnerable to attack
○ That the system is likely vulnerable to attack via the RPC DCOM vulnerability

QUESTION 5 **1 points** ✓ Saved

Which of the following automated methods is most likely to accurately detect a vulnerability on a network?

○ Threat modeling
● Vulnerability analysis (for example, using Retina)
○ Automated hacking (for example, Armitage Hail Mary)
○ Port scanning (for example, a Nmap SYN scan)

QUESTION 6 **1 points** ✓ Saved

If a vulnerability scanner reports that port 80 is open on a Web server, what should you do:

● Nothing, this is normal
○ Use a firewall to block the port
○ Investigate further, it looks like you have malware
○ Change to use a more up-to-date web server, this server is vulnerable to attack

QUESTION 7 **1 points** ✓ Saved

Which of the following would NOT be conducted during a typical vulnerability scan?

○ Service identification on each open port
○ Port scans
○ Probe the system(s), to determine status and configuration of services
● Exploit vulnerabilities

QUESTION 8 **1 points** ✓ Saved

Which of the following is NOT a Vulnerability scanner?

● MSF
○ Nessus
○ OpenVAS
○ None of these
○ Nexpose

QUESTION 9 **1 points** ✓ Saved

OpenVAS is a fork of which project?

○ Nmap
○ Nexpose
● Nessus
○ MSF

QUESTION 10 **1 points** ✓ Saved

Local Web proxies such as Burp Suite or WebScarab are primarily used for:

● Testing a website for security problems, by intercepting requests between an attacker and a server
○ Testing a website for security problems, by intercepting requests between a remote victim and a server
○ Hiding the identity of the attacker
○ Pivoting between compromised servers