COMP623 - Digital Security - 14818 - WIN - 202110
Notifications
Announcements
Module Content
Course Handbook
Assessment & Feedback
Academic Integrity Tutorial
Quote Unquote
Turnitin Student Help
Learning Resources
Reading List
MyBeckett Student Help
Library
Skills For Learning
Module Resources
Module Content
Module Handbook
Quizzes
Report Submission

Take Test: Vulnerabilities

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

A payload that connects back to the attacker and grants them a command line access, is known as a:

- Command shell
- Bind shell
- (•) Reverse shell
- Privilege escalation

QUESTION 2 — 1 points — Saved

A payload that waits for the attacker to connect and grants them command line access, is known as a:

- Reverse shell
- (•) Bind shell
- Privilege escalation
- Command shell

QUESTION 3 — 1 points — Saved

Which of the following is NOT a type of module available in Metasploit Framework (MSF)?

- Post-Exploitation
- Exploit
- Payload
- (•) Malware

QUESTION 4 — 1 points — Saved

What is wrong with the following use of msfconsole?
use exploit/multi/samba/usermap_script
set PAYLOAD cmd/unix/reverse
exploit

- This is not a valid exploit
- This payload is not compatible with this exploit
- (•) The attacker forgot to set options such as IP addresses and ports
- Nothing this will work fine as is

QUESTION 5 — 1 points — Saved

If an attacker starts as a normal user, and ends up as a superuser (root or Administrator). They have managed:

- Buffer overflow
- Horizontal privilege escalation
- (•) Vertical privilege escalation
- Command injection

QUESTION 6 — 1 points — Saved

A method of mitigating the effects of software vulnerabilities is to (best answer):

- Use an IDS
- Use encryption
- (•) Keep software up-to-date
- Install antimalware

QUESTION 7 — 1 points — Saved

A programmer makes a mistake that introduces a security problem. This is known as a(n):

- Exploitation
- Buffer overflow
- Malware
- Shell code
- (•) Software vulnerability
- Exploit
- Payload

QUESTION 8 — 1 points — Saved

A program that takes advantage of a programing mistake to take control of a computer is:

- A Trojan horse
- A network monitor
- (•) An exploit
- A software vulnerability

QUESTION 9 — 1 points — Saved

A small program that takes advantage of a security problem is known as a(n):

- (•) Exploit
- Payload
- Shell code
- Software vulnerability
- Exploitation
- Buffer overflow
- Malware

QUESTION 10 — 1 points — Saved

Which of the following would be most likely to help you to identify any software installed on a machine that was vulnerable to attack via a buffer overflow?

- Vulnerability analysis
- Software patching
- (•) Software updates
- Antimalware