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: Post-exploitation

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	This Test allows 2 attempts. This is attempt number 1.
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

An attacker could use pivoting to:

- (•) All of these
- ( ) Attack systems they could not attack directly
- ( ) Hide their identity
- ( ) Route MSF expliots from one computer through a compromised system to another target

QUESTION 2 — 1 points — Saved

If an attacker attacked a Windows system and obtained a bind shell using Metasploit, which of the following would almost certainly be true?

- ( ) The attacker could modify the Windows kernel
- ( ) The attacker would be able to modify the files of any user
- (•) The attacker would be able to run commands on the Windows system
- ( ) The attacker could modify the software on the system

QUESTION 3 — 1 points — Saved

An exploit that is run as a normal user and is used to obtain superuser access, is known as:

- ( ) a horizontal escalation attack
- ( ) Meterpreter
- (•) a local privilege escalation exploit
- ( ) an arbitrary code execution expliot

QUESTION 4 — 1 points — Saved

If an attacked system is logging to a secure remote server, which of the following methods could be used to effectively cover the tracks of an attacker?

- ( ) All of these
- (•) Disabling logging from the attacked system
- ( ) Modifying log files
- ( ) Deleting log files

QUESTION 5 — 1 points — Saved

On a Windows system, if an attacker has managed to compromise a system, and finds they have a security identifier (SID) of "S-1-5-21-1180699209-877415012-3182924384-500", which of the following will the attacker likely be able to modify?

- ( ) Files belonging to the corresponding user
- ( ) Files owned by any user
- ( ) Any programs or configuration files stored locally
- (•) All of these

QUESTION 6 — 1 points — Saved

Which of the following would give an attacker the ability to do the most amount of damage?

- ( ) A sea shell
- ( ) A bind shell
- (•) A root shell
- ( ) A reverse shell

QUESTION 7 — 1 points — Saved

Port forwarding would be used by an attacker:

- (•) For pivoting attacks through a compromised system
- ( ) For post-exploitation examination of the remote system's hard disk
- ( ) To use up all of a local system's resources, resulting in a DoS
- ( ) As an advanced method of scanning for open ports

QUESTION 8 — 1 points — Saved

Someone monitoring network traffic could easily read all the commands an attacker sends to Meterpreter

- ( ) True
- (•) False

QUESTION 9 — 1 points — Saved

```
msf > use post/linux/gather/checkvm
msf post(checkvm) > show options
msf post(checkvm) > set SESSION 1
msf post(checkvm) > exploit
```

Given this sequence of commands, what has the attacker done?

- ( ) Check whether the attacker has Meterpeter access
- ( ) Run a program on the *attacker's* system to determine whether Kali Linux is running in a VM
- (•) Run a post-exploitation module to gather information from a compromised system
- ( ) Exploited a vulnerability on a remote system, to get a shell

QUESTION 10 — 1 points — Saved

```
msf > use post/linux/gather/hashdump
msf post(checkvm) > set SESSION 1
msf post(checkvm) > exploit
```

Given the above commands, what could an attacker do with the output?

- ( ) This attack won't work, because they forgot to set IP addresses
- ( ) The output is the pain-text passwords! They could try using these credentials to get access to other services
- ( ) They could use the core dump to determine the exact state of the kernel, such as a list of all the current processes on the system
- (•) They could try to crack the hashes