Module 05: Quiz

- Due Feb 28 at 11:59pm
- Points 10
- Questions 5
- Time Limit 10 Minutes

Instructions

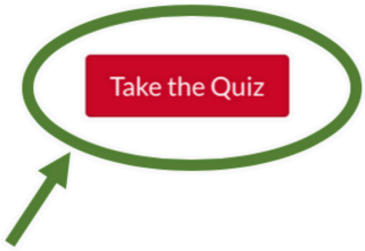
Purpose

This quiz is over the materials for Module 05. This quiz evaluates your ability to parse and decode Ethernet packets and your understanding of countermeasures to mitigate physical network attacks.

Before beginning this quiz, please make sure you have a strong understanding of how to parse packets from your chapter assignment.

Task

DO NOT HIT THE BUTTON UNTIL YOU'RE READY TO TAKE THE QUIZ.



- You may **not** work in groups or with another person.
- You may only take this quiz once.
- Make sure you will not be interrupted so you can focus on completing the quiz.
- Make sure you have a reliable internet connection.
- You have 10 minutes to complete this quiz. Once you start the quiz, you cannot stop the timer.
  - **Pay attention to the time.** The time remaining is located on a timer on the right sidebar.
  - The quiz will *automatically* submit after your time is up or if it hits the due date (whichever comes first).
  - If you accidentally navigate away from the quiz but have time remaining, you should be able to pick up where you left off.

- For multiple select questions (e.g., the 'select all that apply' questions with checkboxes), Canvas auto-grading will reduce the overall score for incorrectly selected options. Unselected options will not alter the score (you won't gain or lose points for not selecting a statement or option, regardless of whether it is correct or incorrect). Be mindful when selecting options for this style of question. See the FAQs page for an example with point values.
- Open book/open notes/open internet - but answers must be your own. Do not copy and do not plagiarize.
- Don't hit the button until you're ready to take the quiz!

Grading Criteria

To complete this assignment, you will answer all of the questions. Canvas will show your scores upon submission. If you have questions about what you missed, please contact your TA.

Solutions

You will be able to see your quiz responses after submitting the quiz. Canvas will show answers with feedback. Please note this feedback and any corrections; you will only see this screen once.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	10 minutes	7 out of 10

ⓘ Correct answers are hidden.

Score for this quiz: 7 out of 10
Submitted Feb 28 at 3:36pm
This attempt took 10 minutes.

Question 1
4 / 4 pts

Answer formatting (same as homework):

- Include any necessary leading zeros (e.g., enter 0101, not just 101).
- Use lowercase letters only.
- Only use 1-9 and a-f in your answer (i.e., no special formatting, do not use 0x prefix).

Packet:

```
6c40 c448 0890 3c5c a132 036d 0800 4500 0034
ac34 0000 3a06 ad44 acd9 092e c0a8 0420 01bb
fc6e 141b 9116 c8fd 5ae9 8010 13a4 228e 0000
0101 080a bff6 6a1c 3f3d 9528
```

For the hex packet above *that has been extracted from the network*, identify the following hex values:

Destination Address: 6c40 c448 0890

Source Address: 3c5c a132 036d

Type/Length: 0800

First 11 bytes of the Data (aka Payload) field: 4500 0034 ac34 00

Answer 1:
6c40 c448 0890
Correct
Answer 2:
3c5c a132 036d
Correct
Answer 3:
0800
Correct
Answer 4:
4500 0034 ac34 0000 3a06 ad
Correct

IncorrectQuestion 2
0 / 2 pts

Consider the following two hex packets *that have been extracted from the network*. Which packet below is an IP packet?

Packet 1

```
4d6d e145 0806 6c40 0889 c448 0800 4500 0034
0000 4000 4006 16bf c0a8 0420 c0e1 9e5b e998
01bb d589 b19f 8760 d615 8010 07fc a52c 0000
0101 080a bdfb 791e b017
```

Packet 2

```
6c40 0889 c448 3c5c 0806 036d
0800 4500 0034 2ec7 4000 3806
eff7 c0e1 9e5b c0a8 0420 01bb
e998 8760 d51d d589 acbe 8010
0046 b317 0000 0101 080a b017
ee65 bdfb 78c6
```

- Only Packet 1

Incorrect. In order to know if it is an IP packet, you must look at the Type/Length field of the Ethernet header. Table 5.2 on page 100 in your textbook shows you common values for this field.

- Only Packet 2
- Both Packets
- Neither Packet

Question 3
2 / 2 pts

Packet:

```
f100 5e5c 91b2 746b 8200 1d8d 8100 0a02
88b5 0081 0000 746b 8200 1d8d 0002 9d7e
4595 0000 0000 000c 00a0 ffff ddff ff19
ffe1 ffff a900 0089 ffff c100 0001
```

Based on the destination address for the packet above, what Ethernet address type does this packet have?

- Unicast

Multicast

Correct. This is a multicast packet. Table 5.3 on page 101 in your textbook shows you the Ethernet address types and their values.

Broadcast

Question 4

1 / 1 pts

Consider a network with VLAN 1 and VLAN 2. If a device is connected to port 3 of a switch means it falls into VLAN 1, then this is an example of...

a static VLAN because port 3 always maps to VLAN 1

Correct. A VLAN where the virtual local area networks are created based on the network ports of the switches and often do not change is a static VLAN. See section 5.4.1 in your textbook.

a dynamic VLAN because any device connected to port 3 will be on VLAN 1

IncorrectQuestion 5

0 / 1 pts

Critical Thinking - Pick the **best** option for the scenario described.

Would a NAC environment be advantageous in an organization that has adopted a bring-your-own-device (BYOD) policy, allowing employees to connect their personal devices, like laptops, to the corporate network?

Yes, it allows for enforcing security policies by blocking any new BYOD from full network access until it complies with specific security requirements, such as installing NAC-approved security applications or the latest security patches.

Yes, it enables the organization to automatically assign limited permissions to BYOD devices and place them into a designated network segment.

Incorrect. All devices grouped together in a NAC environment are given the same permissions. Since the company allows worker to complete their work on their own devices, devices would need access to the network with full permissions for the particular employee, but the company would want to make sure the devices were secure first.

No, because BYOD devices, being personal, cannot directly connect to organizational switches, making NAC unnecessary.

No, because the ownership of BYOD devices is unclear, making it impractical to implement any form of access control.

This question addresses the implementation of a NAC environment in a BYOD context. The correct response, "any new BYOD connected to the network could be blocked until specific criteria in the security policy have been met, such as installing a NAC-approved app or installing the newest security patches," highlights NAC's ability to enforce security policies before allowing devices network access. This is particularly important in a BYOD environment, where a variety of devices with different security postures attempt to connect to the network. The option correctly points out the advantage of ensuring devices meet certain security criteria, which is crucial for maintaining the overall security of the network.

Same quiz reminder:

Upon submission, you will be able to see your quiz responses after submission until you navigate away from the screen. ***Please take notes on your responses, the Canvas feedback, and any corrections, as you will only see this screen once. You will not be able to revisit your quizzes prior to or during your exams.***

If you need help understanding why something is incorrect, please contact Dr. Jacobson or your TA(s). They will be happy to help!

Quiz Score: 7 out of 10