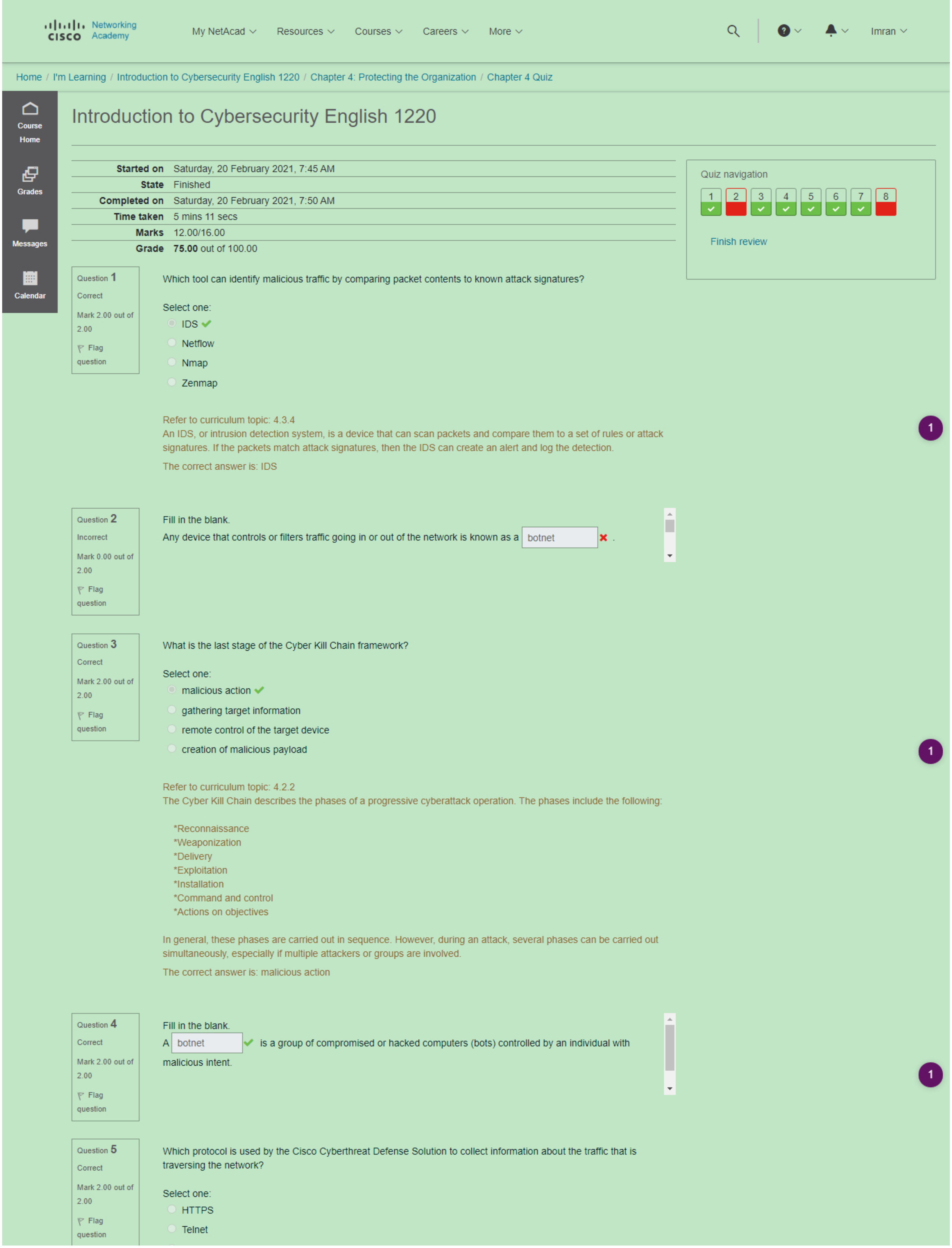


Home / I'm Learning / Introduction to Cybersecurity English 1220 / Chapter 4: Protecting the Organization / Chapter 4 Quiz

Introduction to Cybersecurity English 1220

Started on	Saturday, 20 February 2021, 7:45 AM
State	Finished
Completed on	Saturday, 20 February 2021, 7:50 AM
Time taken	5 mins 11 secs
Marks	12.00/16.00
Grade	**75.00** out of 100.00

Quiz navigation

1	2	3	4	5	6	7	8
✓	🟥	✓	✓	✓	✓	✓	🟥

Finish review

Question **1**
Correct
Mark 2.00 out of 2.00
Flag question

Which tool can identify malicious traffic by comparing packet contents to known attack signatures?

Select one:

● IDS ✓
○ Netflow
○ Nmap
○ Zenmap

Refer to curriculum topic: 4.3.4
An IDS, or intrusion detection system, is a device that can scan packets and compare them to a set of rules or attack signatures. If the packets match attack signatures, then the IDS can create an alert and log the detection.

The correct answer is: IDS

Question **2**
Incorrect
Mark 0.00 out of 2.00
Flag question

Fill in the blank.

Any device that controls or filters traffic going in or out of the network is known as a botnet ✗ .

Question **3**
Correct
Mark 2.00 out of 2.00
Flag question

What is the last stage of the Cyber Kill Chain framework?

Select one:

● malicious action ✓
○ gathering target information
○ remote control of the target device
○ creation of malicious payload

Refer to curriculum topic: 4.2.2
The Cyber Kill Chain describes the phases of a progressive cyberattack operation. The phases include the following:

*Reconnaissance
*Weaponization
*Delivery
*Exploitation
*Installation
*Command and control
*Actions on objectives

In general, these phases are carried out in sequence. However, during an attack, several phases can be carried out simultaneously, especially if multiple attackers or groups are involved.

The correct answer is: malicious action

Question **4**
Correct
Mark 2.00 out of 2.00
Flag question

Fill in the blank.

A botnet ✓ is a group of compromised or hacked computers (bots) controlled by an individual with malicious intent.

Question **5**
Correct
Mark 2.00 out of 2.00
Flag question

Which protocol is used by the Cisco Cyberthreat Defense Solution to collect information about the traffic that is traversing the network?

Select one:

○ HTTPS
○ Telnet

○ NAT

● NetFlow ✓

Refer to curriculum topic: 4.2.3
NetFlow is used both to gather details about the traffic that is flowing through the network, and to report it to a central collector.

The correct answer is: NetFlow

Question **6**

Correct

Mark 2.00 out of 2.00

Flag question

What type of attack disrupts services by overwhelming network devices with bogus traffic?

Select one:

● DDoS ✓

○ port scans

○ zero-day

○ brute force

Refer to curriculum topic: 4.1.3
DDoS, or distributed denial of service, attacks are used to disrupt service by overwhelming network devices with bogus traffic.

The correct answer is: DDoS

Question **7**

Correct

Mark 2.00 out of 2.00

Flag question

Which tool can perform real-time traffic and port analysis, and can also detect port scans, fingerprinting and buffer overflow attacks?

Select one:

○ SIEM

○ Netflow

● Snort ✓

○ Nmap

Refer to curriculum topic: 4.3.4
Snort is an open source intrusion protection system (IPS) that is capable of performing real-time traffic and port analysis, packet logging, content searching and matching, as well as detecting probes, attacks, port scans, fingerprinting, and buffer overflow attacks.

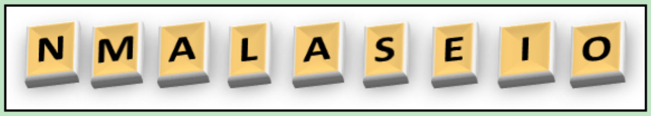
The correct answer is: Snort

Question **8**

Incorrect

Mark 0.00 out of 2.00

Flag question



Refer to the exhibit. Rearrange the letters to fill in the blank.

Behavior-based analysis involves using baseline information to detect anomaly ✖ that could indicate an attack.

Finish review

◄ Chapter 4: Terms and Concepts Practice

Jump to...

Launch Chapter 5 ►