Module 4 Assessment (Attacks & Malicious Code and Activity 3rd)

Due Oct 15 at 11:59pm **Points** 20 **Questions** 20 **Available** Oct 2 at 12am - Oct 16 at 11:59pm **Time Limit** 45 Minutes
Allowed Attempts 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment in the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	21 minutes	18 out of 20

Answers will be shown after your last attempt

Score for this attempt: **18** out of 20
Submitted Oct 10 at 11:26am
This attempt took 21 minutes.

Incorrect

Question 1 — 0 / 1 pts

A computer is periodically checking in with an attacker's command and control center, accepting directions, and then launching attacks on other systems. What is this system called?

- A botnet

- A zombie
- A firewall
- A proxy server

B is correct. Individual systems joined to a botnet are commonly called zombies. A, C, and D are incorrect. The description identifies activity from a botnet, but individual systems are called zombies, and the entire network is called a proxy. Firewalls and proxy servers provide protection and do not launch attacks.

Question 2

1 / 1 pts

You suspect that several systems in your work may be joined to a botnet. What could you check to identify network activity?

- The antivirus software tracking activity in and out of the network
- The antivirus software on each individual system
- (selected) The firewall logs on a network firewall
- The firewall logs on each individual system

C is correct. Because zombies check in with a botnet's command and control center, checking the firewall logs on the network may show these connections. A, B, and D are incorrect. If antivirus software detected the botnet activity, the software should report the activity without taking any additional action. Although it's possible to check the firewall logs on each individual computer, that would be much more time-consuming than checking the firewall logs on the network firewall.

Question 3

1 / 1 pts

A user clicked a link in a phishing e-mail. Afterward, the user's computer periodically sends spam to other computers without the user's knowledge. What has likely occurred?

- The user's system has joined a zombie network
- The user's system has joined a botnet
- The user's e-mail application is malfunctioning
- A logic bomb is running on the user's system

B is correct. These symptoms indicate that the system has joined a botnet and is being controlled by an attacker. A, C, and D are incorrect. The user's system is acting as a zombie in the botnet, but botnets are not called zombie networks. A malfunctioning e-mail application will not send out spam. A logic bomb executes in response to an event, but there's no indication in this case that an event is causing the trigger.

Question 4

1 / 1 pts

A computer is periodically checking in with an attacker's command and control cernter, accepting directions and then launching attacks on other systems. What is directing this computer's activity?

- A botnet
- A zombie
- A firewall

A proxy server

A is correct. This system is part of a botnet and the botnet is directing the system's activity.
B, C, and D are incorrect. Individual systems joined to a botnet are commonly called zombies, but the zombies don't direct the attacking activity. Firewalls and proxy servers provide protection and do not launch attacks.

Question 5

1 / 1 pts

One of the servers in your DMZ has been experiencing a protracted attack from multiple Internet sources, impact its operability. Which of the following best describes this malicious activity?

- DDoS
- botnet
- Insider threat
- Data theft

A is correct. A distributed denial of service (DDoS) attack comes from multiple sources and attempts to reduce a system's ability to respond to legitimate requests for services. When effective, it reduces the operability of the system.
B,C, and D are incorrect. While the DDoS attack may be coming from systems in a botnet, the scenario doesn't give enough information to make that conclusion. An insider threat is from personnel within the organization, such as a disgruntled employee. A data theft results in loss of data, but the scenario doesn't mention data loss.

Question 6

1 / 1 pts

Viruses can often be identified by specific characteristics such as a specific byte pattern with the virus. What is this known as?

- (●) Virus signature
- ( ) Virus fingerprint
- ( ) Virus heuristics
- ( ) Virus language

A is correct. Virus signatures are specific are specific characteristics used to identify the virus. Signature-based antivirus software uses these signatures to detect the viruses.
B, C, and D are incorrect. Although a virus signature is similar to a fingerprint, it is not called a fingerprint. Heuristics are used to detect previously unknown viruses. Viruses can be written in multiple different programming languages, but the specific byte patter isn't known as a virus language.

Question 7

1 / 1 pts

An antivirus program is attempting to detect previously unknown malware. What method of detection is this?

- ( ) Signature-based
- (●) Heuristics-based
- ( ) Characteristics-based
- ( ) Pattern recognition-based

B is correct. Heuristics-based detection attempts to identify previously unknown malware by observing its behavior. This form of detection isolates an application in an area called a sandbox and observes its behavior. A, C, and D are incorrect. Signature-based detection uses a database of known malware identified by specific characteristics or patterns of bytes within the malware.

Question 8

1 / 1 pts

Users in your organization regularly use USB devices, and occasionally a USB device has introduced a virus into the organization. What is the best method of protecting against malware distributed via USBs without affecting the users?

- Scan all spam for viruses
- Use antivirus software
- Prevent the use of USB devices
- Use write-only USB devices

B is correct. The best solution is to use antivirus software.
A, C, and D are incorrect. Although scanning spam for viruses is a good step to take, it only affects viruses spread via e-mail, not USB devices. Preventing the use of USB devices or using write-only USB devices (if such a thing exists) would affect the users.

Question 9

1 / 1 pts

Of the following choices, what could be used to block most of the viruses coming through e-mail?

- A packet filtering firewall
- A proxy server
- A spam filter
- An e-mail server

C is correct. Because most viruses delivered through e-mail come as spam, a spam filter can block most e-mail delivered viruses. Antivirus software is also useful (although it wasn't given as a choice). A, B, and D are incorrect. Neither a packet-filtering firewall no a proxy server can detect malware or spam. An e-mail server is needed to deliver all e-mail and is useful for blocking viruses only if it has a spam filter or antivirus software.

Question 10

1 / 1 pts

Of the following choices, what is the most common method of delivering malware?

- Via floppy disks
- Via USB drives
- Via e-mail
- Through virtual private networks (VPNs)

C is correct. The most common method of delivering malware is over the Internet, such as via spam e-mail.
A, B, and D are incorrect. Floppy drives previously were a common way to spread malware, but such drives are seldom used today. Malware can be delivered via USB drives, but this is not as common as via e-mail. Malware is rarely, if ever, delivered through a VPN.

Question 11

1 / 1 pts

Which of the following statements is true?

- (●) Worms can replicate without user interaction, but viruses cannot replicate without user interaction.
- ( ) Viruses can replicate without user interaction, but worms cannot replicate without user interaction.
- ( ) Trojan horses can replicate without user interaction, but viruses cannot replicate without user interaction.
- ( ) Viruses can replicate without user interaction, but Trojan horses cannot replicate without user interaction.

A is correct. Worms can replicate without user interaction, but viruses need some type of user interaction to replicate.
B, C, and D are incorrect. Viruses and Trojan horses need user interaction to replicate. They cannot replicate without user interaction as a worm can.

Question 12

1 / 1 pts

What type of malware uses encryption to make it more difficult for antivirus researchers to reverse-engineer the code?

- Macro
- Metamorphic
- Polymorphic
- Armored

D is correct. An armored virus uses code to make it difficult for antivirus (AV) researchers to reverse-engineer the code, using techniques such as encryption and polymorphism.
A, B, and C are incorrect. A macro virus resides in a document such as a Microsoft Word or Excel document and does not use encryption. A metamorphic virus mutates the code used to replicate and deliver a payload. A polymorphic virus morphs or mutates each time it replicates to another machine, or even each time it is run. Although a metamorphic virus and polymorphic virus may be encrypted, the purpose of the encryption in these viruses is to escape detection rather than prevent reverse engineering.

Question 13

1 / 1 pts

An organization has installed antivirus software on desktop systems. What else should be done to ensure that new viruses are detected?

- Regularly update virus signatures
- Regularly replace the antivirus software
- Regularly keep the system up to date with patches
- Remove all unneeded protocols

A is correct. Virus signatures should be kept up to date to ensure that new viruses are detected.
B, C, and D are incorrect. It's not necessary to replace the antivirus software regularly, though vendors do update it occasionally. Although it is useful to keep the system up to date with patches and remove unneeded protocols (two steps in hardening a system) these practices do not help to detect new viruses.

Question 14

1 / 1 pts

Of the following, what is NOT used as a stealth method for a virus to hide itself?

- Armor
- Polymorphism
- Metamorphism
- Macro

D is correct. A macro virus resides in a document such as a Microsoft Word or Excel document and is not a method used to hide itself.
A, B, and C are incorrect. Many viruses try to hide themselves from AV software by providing false or misleading information about themselves to the software. Methods used by stealth viruses include using armor, polymorphism, o metamorphism.

Question 15

1 / 1 pts

What type of virus has multiple components?

- Macro
- Multipartite
- Armored
- Polymorphic

B is correct. A multipartite virus has multiple components. For example, it could combine a boot sector virus with a virus that infects one or more files.
A, C, and D are incorrect. A macro virus resides in a document such as a Microsoft Word or Excel document. An armored virus uses code to make it difficult for AV researchers to reverse-engineer the code. A polymorphic virus has the ability to morph or mutate each time that it replicates to another machine or even each time it runs.

Question 16

1 / 1 pts

What is a distinct difference between a virus and a worm?

- A virus is executed through user interaction and a worm does not require user interaction.
- A worm is executed through user interaction and a virus does not require user interaction.
- A virus is executed in response to an event and worm does not have an event trigger.
- A virus is executed through user interaction and a worm is executed in response to an event.

A is correct. A virus can run only with some type of user interaction. Typically the interaction is a user running a program, but it could be a user inserting a USB drive into a system. A worm does not require user interaction.
B, C, and D are incorrect. A worm does not need user interaction to execute. A logic bomb (not a virus or worm) executes in response to an event.

Question 17

1 / 1 pts

Of the following choices, what does NOT represent a function of a content-filtering appliance?

- Filtering spam going into a network
- Filtering malware going into a network
- Providing proxy server services
- Acting as a honeypot

D is correct. A honeypot is a server with fake content designed to attract an attacker. It is not part of a content-filtering appliance.
A, B, and C are incorrect. A content-filtering appliance can filter spam and malware and provide proxy server services.

Question 18

1 / 1 pts

A user notices suspicious activity on a computer and suspects that it may have malware installed. What should be done first?

- Perform a real-time scan
- Perform an on-demand scan
- Perform a scheduled scan
- Update the signatures

D is correct. A scan is appropriate, but prior to the scan, the virus signatures should be updated.
A, B and C are incorrect. A real-time scan provides protection continuously when a user opens a file. An on-demand scan is appropriate in this case, but only after updating the virus signatures. A scheduled scan occurs on a regular basis.

Incorrect

Question 19

0 / 1 pts

Which of the following is NOT a valid method of preventing infection from malware?

- Implementing least privilege
- Educating users
- Installing antivirus software
- Ensuring that antivirus definitions are not modified

D is correct. Antivirus signature definitions should be regularly updated to detect new viruses.
A, B, and C is incorrect. Implementing a principle of least privilege, educating users about malware, and installing antivirus software are all valid methods of helping to prevent malware infection.

Question 20

1 / 1 pts

Which of the following statements is true about spyware?

- It appears to be one thing but is something else
- It is software that can install on a user's system without the user's knowledge or consent
- It travels over a network and installs itself on computers without user interaction
- It cannot be detected by antivirus software

B is correct. Spyware is software that can install itself on a user's system without the user's knowledge or consent. A, C, and D are incorrect. A Trojan horse (not spyware) appears to be one thing but is something else. A worm (not spyware) travels over a network and installs itself on computers without user interaction. Most antivirus software includes the ability to search for and detect spyware.

Quiz Score: **18** out of 20