Knowledge Check Quiz Related Topic Week 6 (Malware Incident Prevention)

Due Feb 27 at 11:59pm **Points** 18 **Questions** 18
Available until Feb 27 at 11:59pm **Time Limit** None

Instructions

Answer the following questions on the related topic material this week.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	14 minutes	18 out of 18

Score for this quiz: **18** out of 18
Submitted Jan 24 at 12:13pm
This attempt took 14 minutes.

Question 1

1 / 1 pts

What is the term for malware that is self-contained and non-replicating that appears benign but has hidden malicious purpose?

Correct!

- (selected) Trojan Horse
- Backdoor
- Worm
- Attacker Toolkit

Question 2

1 / 1 pts

What is the term for an attack method that tricks people into revealing sensitive information?

- Malicious Mobile Code
- Social Engineering

Correct!

- Rootkit
- Signature

Question 3

1 / 1 pts

What is the term for malware that listens for commands on a certain port?

- Trojan Horse
- On-Access Scanning
- Backdoor

Correct!

- Phishing

Question 4

1 / 1 pts

What is the term for fraudulent emails intended to deceive users into disclosing personal data?

- Backdoor

Correct!

- Phishing
- Signature
- Rootkit

Question 5

1 / 1 pts

What is the term for the attacker tool that monitors and records keyboard use?

- Attacker Toolkit
- Mobile Code

Correct!

- Keystroke Logger
- Social Engineering

Question 6

1 / 1 pts

What is the term for software with malicious intent transmitted from a remote host?

- Keystroke Logger
- Attacker Toolkit
- Social Engineering

Correct!

- Malicious Mobile Code

Question 7

1 / 1 pts

What is the term for a set of characteristics of known malware instances that can be used to identify malware?

Correct!

- Signature
- Quarantine
- On-Demand Scanning
- Social Engineering

Question 8

1 / 1 pts

What is the term for a collection of files installed to alter functionality in a malicious and stealthy way?

- Backdoor
- Phishing

Correct!

- Rootkit
- Signature

Question 9

1 / 1 pts

What is the term for a controlled environment that isolates the application and restricts what operations the applications can perform?

- Trojan Horse
- Sandbox

Correct!

- Rootkit
- Backdoor

Question 10

1 / 1 pts

What is the term for the collection of utilities and scripts used to probe and attack hosts?

- On-Access Scanning
- Attacker Toolkit

Correct!

- Social Engineering
- Antivirus Software

Question 11

1 / 1 pts

What is the difference between a **virus** and a **worm**?

Correct!

- (selected) Both are self-replicating, but a worm self-replicates without user intervention
- A virus self-replicates and a worm is non-replicating.
- Both are self-replicating, but a virus self-replicates without user intervention
- A worm self-replicates and a virus is non-replicating.

Question 12

1 / 1 pts

What is the difference between quarantining and disinfecting files?

- Quarantine is for suspected malware and disinfection is for known malware
- Quarantine removes malware from within a file

Correct!

- (selected) Quarantine contains malware files in isolation
- Disinfection stores files containing malware for future quarantine

Question 13

1 / 1 pts

Which malware incident prevention practice relates to **policy**?

Correct!

- (selected) Restrict the use of removable media

- Eliminate unsecured file shares
- Not opening suspicious emails or attachments
- Scan files for known malware

Question 14

1 / 1 pts

Which malware incident prevention practice relates to **awareness**?

- Restrict the use of removable media
- Scan files for known malware
- Eliminate unsecured file shares

Correct!

- Not opening suspicious emails or attachments

Question 15

1 / 1 pts

Which malware incident prevention practice relates to **vulnerability mitigation**?

- Scan files for known malware

Correct!

- Eliminate unsecured file shares
- Not opening suspicious emails or attachments
- Restrict the use of removable media

Question 16

1 / 1 pts

Which malware incident prevention technique is an example of **threat mitigation**?

- Sandboxing
- BIOS Protection
- Browser Separation

Correct!

- Intrusion Prevention Systems

Question 17

1 / 1 pts

Which malware incident prevention technique is an example of **defensive architecture**?

- Application Whitelisting
- Content Filtering/Inspection
- Antivirus Software

Correct!

- Segregation through Virtualization

Question 18

1 / 1 pts

Which incident response phase relates to **identifying malware incident characteristics**?

- Preparation
- Post-Incident Activity

Correct!

- (selected) Detection & Analysis
- Containment Eradication & Recovery

Quiz Score: **18** out of 18