Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 7:59:15 pm • Time spent: 00:30

Score: 0% Passing Score: 80%

Question 1: ✕ Incorrect

Which common design feature among instant messaging clients make them less secure than other means of communicating over the internet?

- Freely available for use
- Peer-to-peer networking
- Real-time communication
- Transfer of text and files

EXPLANATION

The common design feature among instant messaging clients that makes them less secure than other means of communicating over the internet is their use of peer-to-peer networking. Peer-to-peer networking is inherently less secure than traditional client/server communication or networking mechanisms. With peer-to-peer networking, there is no centralized access control authority, so any client on the system can introduce malicious code or perform malicious actions without restriction.

The other design features listed here are typically seen as strengths of instant messaging clients rather than as aspects of insecurity or vulnerability.

REFERENCES

5.10.3 Network Application Facts

q_net_app_peer_01_secp7.question.fex

Question 2: ✕ Incorrect

Which type of application allows users to share and access content without using a centralized server?

- Instant messaging
- Group Policy
- Peer-to-peer software
- Real-time communication

EXPLANATION

Peer-to-peer software allows users to share content and access content shared by other users without using centralized servers or centralized access control.

Instant messaging provides real-time text messaging communication and supports picture, music, and document exchange.

Group Policy defines security options on a Windows operating system.

Real-time communication is a strength of instant messaging clients.

REFERENCES

5.10.3 Network Application Facts

q_net_app_peer_02_secp7.question.fex

Question 3: ✕ Incorrect

Which of the following methods did Microsoft introduce in Windows 10 to help distribute OS updates?

- File Transfer Protocol
- Peer-to-peer software
- Server download
- Group Policy

EXPLANATION

Peer-to-peer software allows users to share content and access content shared by other users without using centralized servers or centralized access control. Microsoft introduced a P2P component to help with distributing OS updates in Windows 10.

File Transfer Protocol is used to transfer files, but was not introduced in Windows 10 to help with distributing OS updates.

Group Policy is used to define security policies on a Windows operating system.

Server download is the traditional model of downloading a file or application. It was not introduced in Windows 10 to help distribute OS updates.

REFERENCES

5.10.3 Network Application Facts

q_net_app_peer_03_secp7.question.fex

Question 4: ✕ Incorrect

Which of the following is a benefit of P2P applications?

- ➡ Shared resources
- Strong security
- Real-time communication
- Low-upload bandwidth

EXPLANATION

Peer-to-peer (P2P) software allows users to share content and access content shared by other users without using centralized servers or centralized access control. Peer-to-peer applications can be a great way to share bandwidth and resources.

Strong security is not a benefit of P2P applications. Many of these applications pose high security risks.

Real-time communication is a strength of instant messaging clients.

Low-upload bandwidth is not a benefit of P2P applications. P2P applications consume large amounts of upload bandwidth.

REFERENCES

5.10.3 Network Application Facts

q_net_app_peer_04_secp7.question.fex

Question 5: ✕ Incorrect

What do application control solutions use to identify specific applications?

- Packet inspection
- ➡ Application signatures
- Flags
- Whitelists

EXPLANATION

Application control implementations use application signatures to identify specific applications.

Group Policy is used to define security policies on a Windows operating system. Application control systems do not use group policies to identify specific applications.

Whitelists are used to define which applications are allowed on network devices.

Packet inspection is performed by firewalls, not application control solutions.

REFERENCES

5.10.3 Network Application Facts

7.2.3 Combining Cryptographic Methods

7.2.5 Cryptographic Implementation Facts

q_net_app_signature_secp7.question.fex

Question 6: ✕ Incorrect

Which of the following is susceptible to social engineering exploits?

- Real-time communication
- Group Policy
- Peer-to-peer software
- ➡ Instant messaging

EXPLANATION

Instant messaging applications can be a vehicle for malware and virus delivery as well as social engineering exploits.

Peer-to-peer (P2P) software allows users to share content and access content shared by other users without using centralized servers or centralized access control.

Group Policy is used to define security policies on a Windows operating system.

Real-time communication is a strength of instant messaging clients.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 5.10.3 Network Application Facts

q_net_app_social_secp7.question.fex

Question 7: ✕ Incorrect

Which of the following is considered a major problem with instant messaging applications?

- Transfer of text and files
- Real-time communication
- ➡ Loss of productivity
- Freely available for use

EXPLANATION

While instant messaging applications offer a quick way to communicate, loss of productivity is considered one of the major problems with these applications.

The other design features listed here are typically seen as strengths of instant messaging clients rather than as aspects of security or vulnerability.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 5.10.3 Network Application Facts

q_net_app_spim_01_secp7.question.fex

Question 8: ✕ Incorrect

You are the security analyst for your organization and have recently noticed a large amount of spim on the company mobile devices. Employees rely on the IM app to communicate with each other.

Which of the following countermeasures should you implement?

- Create a blacklist.
- Disable instant messaging.
- Encrypt all IM traffic.
- Use an IM blocker.

EXPLANATION

Spim is a type of spam that targets users of instant messaging services. Creating a whitelist or using an IM blocker are countermeasures that can be implemented against spim.

Creating a blacklist does not help much against spim.

Disabling instant messaging would stop the spim, but this would also stop employees from communicating with each other.

Encrypting IM traffic would not stop the spim messages.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 5.10.3 Network Application Facts

q_net_app_spim_02_secp7.question.fex

Question 9: ✕ Incorrect

You have implemented a new application control solution. After monitoring traffic and use for a while, you have noticed an application that continuously circumvents blocking.

How should you configure the application control software to handle this application?

- Tarpit
- Drop
- Flag
- Block

EXPLANATION

When using tarpit, the connection between hosts is kept alive while the application data itself is silently dropped. This makes it appear to both hosts that the other host is receiving the data but is not responding. Some malicious applications notice they are being blocked and circumvent the issue. Using tarpit prevents the application from realizing it has been blocked and stops it from circumventing security controls.

Blocked applications are not allowed and are blocked. The session is dropped if it uses UDP and is reset if it uses TCP.

Flagged applications are allowed, but a violation is logged when they are identified.

Drop is not a application control software configuration option.

REFERENCES

5.10.3 Network Application Facts

q_net_app_tarpit_secp7.question.fex

Question 10: ✕ Incorrect

You are implementing a new application control solution.

Prior to enforcing your application whitelist, you want to monitor user traffic for a period of time to discover user behaviors and log violations for later review.

How should you configure the application control software to handle applications not contained in the whitelist?

- Drop
- Tarpit
- Block
- ➡ Flag

EXPLANATION

When using an application control solution, an application whitelist is defined centrally and applied to all network devices. Only applications contained in the whitelist are allowed. Applications not whitelisted can have several actions applied:

- Blocked applications are not allowed. The session is dropped if it uses UDP and reset if it uses TCP.
- Flagged applications are allowed, but a violation is logged when they are identified.
- Tarpitted applications are not allowed. However, the connection between hosts is kept alive while the application data itself is silently dropped. This makes it appear to both hosts that the other host is receiving the data but not responding.

Not all application control solutions support tarpitting application traffic.

REFERENCES

5.10.3 Network Application Facts

q_net_app_white_secp7.question.fex