Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/22/2022 1:47:35 pm • Time spent: 01:50

Score: 90% Passing Score: 80%

Question 1: ✔ Correct

You have been receiving a lot of phishing emails sent from the domain kenyan.msn.pl. Links within these emails open new browser windows at youneedit.com.pl.

You want to make sure that these emails never reach your inbox, but you also want to make sure that emails from other senders are not affected.

What should you do?

- ➡ Add **kenyan.msn.pl** to the email blacklist.
- Add **pl** to the email blacklist.
- Add **youneedit.com.pl** to the email blacklist.
- Add **msn.pl** to the email blacklist.

EXPLANATION

Add **kenyan.msn.pl** to the email blacklist. Adding **msn.pl** or **pl** to the blacklist filters out all emails from kenyan.msn.pl, but this also filters out other emails from the msn.pl or pl domains. Adding **youneedit.com.pl** to the email blacklist would prevent emails from that domain, but it would not prevent emails from kenyan.msn.pl, nor would it prevent links in the emails from opening windows to youneedit.com.pl.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_blacklist_secp7.question.fex

Question 2: ✔ Correct

You install a new Linux distribution on a server in your network. The distribution includes a Simple Mail Transfer Protocol (SMTP) daemon that is enabled by default when the system boots. The SMTP daemon does not require authentication to send email messages.

Which type of email attack is this server susceptible to?

- Phishing
- Sniffing
- Open SMTP relay
- Viruses

EXPLANATION

An SMTP relay is an email server that accepts mail and forwards it to other mail servers, and an open SMTP relay allows anyone to forward mail if they choose. If your mail server is an open SMTP relay, spammers can also take advantage of it to obscure the actual source of the email. If spammers use your relay for sending mail, your server may soon be placed on a blacklist. Other mail servers will then stop receiving any mail (even legitimate mail) sent from your servers. As a best practice:

- Configure your mail server to accept mail only from authenticated users or specific email servers that you authorize.
- Require TLS encryption to connect to the server.

A phishing scam uses an email pretending to be from a trusted organization that asks you to verify personal information or send money. Sniffing occurs when a user captures packets from a network and inspects their contents. Viruses are types of malware that spread by infecting legitimate files on a computer system and are sometimes sent as email attachments.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_email_secp7.question.fex

Question 3: ✔ Correct

Which of the following BEST describes an email security gateway?

- It provides a form of identity verification.
- It accepts mail and forwards it to other mail servers.
- It requires the use of a public key certificate.
- ➡ It monitors emails that originate from an organization.

EXPLANATION

An email security gateway is a security solution that monitors emails that are sent to or originate from an organization.

Email encryption digitally signs an email with a certificate. The certificate provides a form of identity verification.

The important thing to understand about Secure/Multipurpose Internet Mail Extensions (S/MIME) is that it requires the use of a public key certificate in order to encrypt and decrypt email messages.

An SMTP relay is an email server that accepts mail and forwards it to other mail servers.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_gateway_secp7.question.fex

Question 4: ✔ Correct

Users in your organization receive email messages informing them that suspicious activity has been detected on their bank accounts. They are directed to click a link in the email to verify their online banking username and password. The URL in the link is in the .ru top-level DNS domain.

Which kind of attack has occurred?

- Buffer overflow
- Virus
- Phishing
- Open SMTP relay

EXPLANATION

A phishing scam uses an email that purports to be from a trusted organization and asks you to verify personal information or send money. In a phishing attack:

- A fraudulent message (which appears to be legitimate) is sent to a target.
- The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and web pages look almost identical to legitimate requests from legitimate websites.
- The fraudulent website requests that the victim provide sensitive information, such as an account number and password.

An SMTP relay is an email server that accepts mail and forwards it to other mail servers. In a buffer overflow attack, a program (while writing data to a memory buffer) overruns the buffer's boundaries and writes data in adjacent memory addresses.

REFERENCES

1.2.3 Defense Planning Facts

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

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

q_email_sec_phishing_01_secp7.question.fex

Question 5: ✔ Correct

Which of the following BEST describes phishing?

- Unwanted and unsolicited email sent to many recipients.
- An email server that accepts mail and forwards it to other mail servers.
- Malware that often uses email as its distribution mechanism.
- A fraudulent email that claims to be from a trusted organization.

EXPLANATION

Phishing is a fraudulent email that claims to be from a trusted organization.

Spam is unwanted and unsolicited email sent to many recipients.

A virus is malware that often uses email as its distribution mechanism.

An SMTP relay is an email server that accepts mail and forwards it to other mail servers.

REFERENCES

1.2.3 Defense Planning Facts

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

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

q_email_sec_phishing_02_secp7.question.fex

Question 6: ✔ Correct

Which of the following would you do to help protect against phishing?

- In the email client, disable preview screens.
- Don't click on an unsubscribe link at the bottom of an unsolicited email.
- Only open emails if you recognize the sender.
- Don't post your full email address anywhere on the web.

EXPLANATION

To protect against phishing:

- Check the email header information to see more info about the sender and the links that are in the email.
- Only open emails if you recognize the sender.
- Check the actual link destination within emails to verify that they go to the correct URL and not a spoofed one.
- Do not click on links in emails. Instead, type the real URL into the browser. You could also look up the website in a search engine.
- Verify that HTTPS is used when going to e-commerce sites. HTTPS requires a certificate that matches the server name in the URL that is verified by a trusted certificate authority (CA). You can also look for the lock icon to verify that HTTPS is used.
- Implement phishing protections within your browser.

To control spam:

- Enable spam filters on client and email servers. Filter junk email by identifying safe senders (whitelists), blocked senders (blacklists), countries to block email from, and languages to block.
- Enable antivirus scanning for attachments on the client and email servers.
- In the email client, disable preview screens. An email can have links for active items that can report back to the spammer.
- Don't click on an unsubscribe link at the bottom of an unsolicited email. Doing this verifies to the spammer that the email address is a current and active email address. Only unsubscribe from trusted organizations.
- Install server-level, anti-spam software on the email server.
- Don't post your full email address anywhere on the web. Spammers use software to scan websites to find email addresses and then add them to their email lists for spamming.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_phishing_03_secp7.question.fex

Question 7: ✕ Incorrect

Which of the following mechanisms can you use to add encryption to email? (Select two.)

- [x] ~~Secure Shell~~
- [ ] HTTPS
- [ ] PGP
- [x] S/MIME
- [ ] Reverse DNS

EXPLANATION

Use Pretty Good Privacy (PGP) or Secure MIME (S/MIME) to add encryption to emails.

HTTPS is used by web browsers to request data from web servers. Secure Shell (SSH) is a secure remote management utility. Reverse DNS can be used to verify the sending device's IP address included in an email. However, this does not add encryption to email messages.

REFERENCES

13.3.2 Email Security Facts

q_email_sec_smime_secp7.question.fex

Question 8: ✔ Correct

If an SMTP server is not properly and securely configured, it can be hijacked and used maliciously as an SMTP relay agent. Which activity could result if this happens?

- Data diddling
- Virus hoax
- Salami attack
- Spamming

EXPLANATION

Attackers often distribute spam by hijacking a misconfigured SMTP server. SMTP servers that act as relay agents for unauthorized or external users can be easily employed to deliver spam. It is extremely important to properly configure SMTP servers to accept email only from authorized internal users.

A salami attack is an attack where small amounts of information, data, or valuables are taken over a period of time. The result is to construct or obtain data or property of great value. A common example of a salami attack is to deposit the fractions of cents from an accounting program into a numbered account. Eventually, the fraction deposits total a significant sum. Data diddling is changing information during input, processing, output, or storage. A virus hoax is a social engineering attack designed to play off of the fears of victims to convince them to perform malicious activities against themselves.

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

5.6.1 Web Threat Protection

5.6.1 Web Threat Protection

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

13.3.3 Protecting a Client from Spam

q_email_sec_spam_01_secp7.question.fex

Question 9: ✔ Correct

Which type of malicious activity can be described as numerous unwanted and unsolicited email messages sent to a wide range of victims?

- Hijacking
- Brute force
- ➡ Spamming
- Trojan horse

EXPLANATION

Spamming is a type of malicious activity can be described as numerous unwanted and unsolicited email messages being sent to a wide range of victims. Spam itself is not usually malicious in nature. More often than not, it is advertising for some product or service. Unfortunately, spam accounts for 40 to 60 percent of all email traffic on the internet. Most of this activity is unsolicited.

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
- 5.6.1 Web Threat Protection
- 5.6.4 Web Threat Protection Facts
- 13.3.2 Email Security Facts
- 13.3.3 Protecting a Client from Spam

q_email_sec_spam_02_secp7.question.fex

Question 10: ✔ Correct

An attacker sends an unwanted and unsolicited email message to multiple recipients with an attachment that contains malware.

Which kind of attack has occurred in this scenario?

- Repudiation attack
- Open SMTP relay
- Phishing
- ➡ Spam

EXPLANATION

Spam is unwanted and unsolicited email messages sent to many recipients. Spam:

- Can be benign, such as emails trying to sell products.
- Can be malicious, such as emails containing phishing content, drive-by downloads, or malware.
- Can contain malware as attachments.
- Wastes bandwidth and could fill an inbox, resulting in a denial-of-service condition.

An open SMTP relay allows anyone to forward mail. An open SMTP relay can be used by spammers to send mail. A phishing scam is an email pretending to be from a trusted organization, asking the recipient to verify personal information or send money. In a repudiation attack, an attacker accesses your email server and sends spoofed emails to others, making them appear as if they came from you.

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

5.6.1 Web Threat Protection

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

13.3.3 Protecting a Client from Spam

q_email_sec_spam_03_secp7.question.fex