Exam Report: 7.10.8 Practice Questions

Date: 1/23/2020 12:56:16 pm
Time Spent: 3:19

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

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

- Spamming
- Virus hoax
- Data diddling
- Salami attack

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

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_01]

Question 2: Correct

Which of the following could easily result in a denial of service attack if the victimized system had too little free storage capacity?

- Spam
- Impersonation
- Sniffing
- Replay attack

Explanation

Spam could easily result in a denial of service attack if the victimized system had too little free storage capacity. If too much spam is received by a system that does not have automatic filters or before a human can identify and purge spam, it is possible to consume all available storage space on the system and cause a system shutdown. This is a type of denial of service attack.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_02]

Question 3: Incorrect

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 want to make sure that emails from other senders are not affected.

What should you do?

- ~~Add **youneedit.com.pl** to the email blacklist~~
- Add **pl** to the email blacklist
- Add **kenyan.msn.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 will filter out all emails from **kenyan.msn.pl**, but will also filter 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 would not prevent emails from **kenyan.msn.pl**, nor would it prevent links in the -mail from opening windows to **youneedit.com.pl**.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_03]

Question 4: Correct

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

- Brute force
- Spamming
- Trojan horse
- Hijacking

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 the email traffic on the internet. Most of this activity is unsolicited.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_04]

Question 5: Correct

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

What kind of attack has occurred in this scenario?

- Repudiation attack
- Open SMTP relay
-

Spam

Phishing

Explanation

Spam is unwanted and unsolicited email 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 the 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, the attacker accesses your email server and sends spoofed emails to others, making them appear as if they came from you.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_05]

Question 6: Correct

What is the most common means of virus distribution?

Floppy disks

Commercial software CDs

Music downloaded from the internet

Email

Explanation

Email is the most common means of virus distribution. Often, viruses employ self-contained SMTP servers to facilitate self-replication and distribution over the internet. Viruses are able to spread quickly and broadly by exploiting the communication infrastructure of internet email. For this reason, it is important to keep your anti-virus software updated so as to block any possible attempt of viruses to infect your systems or to spread to other systems.

Floppy disks, downloaded music files, and commercial software CDs all have the potential to spread viruses, but they are not as common as email.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_08]

Question 7: Correct

You install a new Linux distribution on a server in your network. The distribution includes an 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

Viruses

Open SMTP relay

Explanation

An *SMTP relay* is an email server that accepts mail and forwards it to other mail servers. An open SMTP relay allows anyone to forward mail. If your mail server is an open SMTP relay, spammers can use it to send mail. Spammers use your relay to obscure the actual source of the email. If spammers use your

relay for sending mail, your server will 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 the 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

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_09]

Question 8: 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 user name and password. The URL in the link is in the .ru top-level DNS domain.

What kind of attack has occurred?

- ○ Buffer overflow
- ○ Open SMTP relay
- ○ Virus
- ➡ ◉ Phishing

Explanation

A *phishing* scam uses an email pretending 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 boundary and writes data in adjacent memory addresses.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_10]

Question 9: Incorrect

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

- ➡ ☑ S/MIME
- ➡ ☐ PGP
- ☐ Secure Shell
- ☐ Reverse DNS
- ☐ HTTPS

Explanation

Use PGP (Pretty Good Privacy) or S/MIME (Secure MIME) to add encryption to emails.
HTTPS is used by web browsers to request data from web servers. Secure Shell is a secure remote management utility. Reverse DNS can be used to verify the sending device IP address included in an email, but does not add encryption to email messages.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_06]

Question 10: Correct

You want to use a protocol for encrypting emails that uses a PKI with X.509 certificates. Which method should you choose?

- AES
- IPsec
- SSH
- S/MIME

Explanation

Secure/Multipurpose Internet Mail Extensions (S/MIME) uses certificates issued by either public or in-house CAs using the X.509 system.

AES encryption is used to encrypt wireless networks using WPA2. SSH is used for secure remote administration and is used to add security to other protocols. IPsec is a method for encrypting network traffic.

References

LabSim for Security Pro, Section 7.10.
[All Questions SecPro2017_v6.exm EMAIL_07]