Exam Report: 5.8.5 Practice Questions

Date: 1/21/2020 10:26:10 am
Time Spent: 3:50

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following is a valid security measure to protect email from viruses?

- Use PGP to sign outbound email
- Limit attachment size to a maximum of 1 MB
- Use reverse DNS lookup
- Use blockers on email gateways

Explanation

The only effective security measure against email viruses is to use virus blockers on email gateways.

Reverse DNS lookup protects against source address spoofing. Using PGP to sign outbound email does not affect inbound email that could contain viruses. Limiting attachment size is ineffective as well, because many viruses are simple scripts that are very small.

References

LabSim for Security Pro, Section 5.8.
[All Questions SecPro2017_v6.exm WEB_THREAT_PROT_01]

Question 2: Correct

Which of the following prevents access based on website ratings and classifications?

- NIDS
- Content filter
- DMZ
- Packet-filtering firewall

Explanation

An internet *content filter* is software used to monitor and restrict what content is delivered across the web to an end user. Companies, schools, libraries, and families commonly use content filters to restrict internet access, block specific websites, or block specific content.

A packet-filtering firewall examines the packet header information to make forwarding decisions. The firewall can accept or reject packets based on IP address, but not individual websites. A network-based IDS (NIDS) is a dedicated device installed on the network. It analyzes all traffic on the network, looking for potential attacks. A demilitarized zone (DMZ) is a buffer network (or subnet) that sits between the private network and an untrusted network, such as the internet.

References

LabSim for Security Pro, Section 5.8.

[All Questions SecPro2017_v6.exm WEB_THREAT_PROT_02]

Question 3: Incorrect

Drag the web threat protection method on the left to the correct definition on the right.

Prevents users from visiting malicious websites

~~URL content filtering~~ Web threat filtering

Prevents outside attempts to access confidential information

✓ Anti-phishing software

Identifies and disposes of infected content

✓ Virus blockers

Prevents unwanted email from reaching your network

✓ Gateway email spam blockers

Prevents users from visiting restricted websites

~~Web threat filtering~~ URL content filtering

Explanation

- *Web site/URL content filtering* prevents users from visiting restricted websites.
- *Web threat filtering* prevents users from visiting websites with known malicious content.
- *Gateway e-mail spam blockers* prevent spam email from reaching your network, servers, and computers.
- *Virus blockers*, often coupled with email blockers, identify infected content and dispose of it.
- *Anti-phishing software* scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

References

LabSim for Security Pro, Section 5.8.
[All Questions SecPro2017_v6.exm WEB_THREAT_PROT_03]

Question 4: Incorrect

You are investigating the use of website and URL content filtering to prevent users from visiting certain websites.

Which benefits are the result of implementing this technology in your organization? (Choose two.)

- ☐ Identification and disposal of infected content
- ➡ ☑ Enforcement of the organization's internet usage policy
- ➡ ☐ An increase in bandwidth availability
- ☐ Prevention of emails containing threats
- ☑ ~~Prevention of phishing attempts~~

Explanation

Website filtering can be used to enforce the organization's internet usage policy and usually results in an increase in bandwidth availability.

Spam blockers are used to block emails containing threats. Virus blockers identify infected content and dispose of it. Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

References

LabSim for Security Pro, Section 5.8.
[All Questions SecPro2017_v6.exm WEB_THREAT_PROT_04]

Question 5: Incorrect

Which of the following are functions of gateway email spam blockers? (Select two.)

- [x] ~~Blocks phishing attempts, which try to access confidential information~~
- [ ] Filters messages containing specific content
- [ ] Blocks users from visiting websites with malicious content
- [ ] Helps enforce an organization's internet usage policy
- [x] Blocks email from specific senders

Explanation

Gateway email spam blockers can be used to block the following:

- Messages from specific senders
- Email containing threats (such as false links)
- Messages containing specific content

Web threat filtering prevents users from visiting websites with known malicious content. Website and content filtering can be used to enforce the organization's internet usage policy. Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outsiders from accessing confidential information.

References

LabSim for Security Pro, Section 5.8.
[All Questions SecPro2017_v6.exm WEB_THREAT_PROT_05]