Exam Report: 13.6.10 Practice Questions

Date: 4/15/2020 4:44:36 pm
Time Spent: 3:02

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

Joe, a user, receives an email from a popular video streaming website. The email urges him to renew his membership. The message appears official, but Joe has never had a membership before. When Joe looks closer, he discovers that a hyperlink in the email points to a suspicious URL.

Which of the following security threats does this describe?

○ Zero-day attack

○ Man-in-the-middle

➡ ● Phishing

○ Trojan

Explanation

Phishing is an attempt to trick a user into compromising personal information or downloading malware. Most often, it involves an email containing a malicious attachment or hyperlink.

A man-in-the-middle (MITM) attack intercepts communications between two systems and alters the message before sending it on to the original recipient. A zero-day attack is an exploit of an operating system or software vulnerability that is unknown and unpatched by the author. A Trojan horse, or Trojan, is a type of malware that is often disguised as legitimate software.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_03]

Question 2: Correct

A large number of compromised computers are infected with malware that allows an attacker (herder) to control them to spread email spam and launch denial-of-service attacks.

Which of the following does this security threat describe?

○ Man-in-the-middle

➡ ● Zombie/botnet

○ Phishing

Explanation

Devices that are infected with malware that can be remote controlled by an attacker are known as zombies. A collection of these zombies that are controlled by the same attacker are known as a botnet (robot network).

Phishing is an attempt to trick a user into compromising personal information or downloading malware. Most often, it involves an email containing a malicious attachment or hyperlink. A man-in-the-middle (MITM) attack intercepts communications between two systems and alters the message before sending it on to the original recipient. Spoofing is when an entity misrepresents itself by using a fake IP address or, more commonly, a fake email address that resembles a real address. The person being spoofed may not immediately discover that the address is fake.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_04]

▼ **Question 3:** Correct

What is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously?

○ Ransomware

○ Worm

○ Scareware

➡ ● Trojan

Explanation

A Trojan horse is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously. Trojan horses are commonly internet downloads. To keep your systems secure and free from such malicious code, you need to take extreme caution when downloading any type of file from just about any site on the internet. If you don't fully trust the site or service that is offering a file, don't download it.

A worm is a type of malicious code similar to a virus. A worm's primary purpose is to duplicate itself and spread, while not necessarily intentionally damaging or destroying resources. Ransomware is a form of malware that denies access to an infected computer system until the user pays a ransom. Scareware is a scam that fools users into thinking they have some form of malware on their system. The intent of the scam is to sell the user fake antivirus software to remove malware they don't have.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_05]

▼ **Question 4:** Correct

○ It is a program that attempts to damage a computer system and replicate itself to other computer systems.

➡ ● It monitors the actions you take on your machine and sends the information back to its originating source.

○ It monitors the actions of the user and then sends pop-up ads to the user that match their tastes.

○ It is a malicious program that is disguised as legitimate software.

Explanation

Spyware monitors the actions you take on your machine and sends the information back to its originating source.

Adware monitors the actions of the user that would denote their personal preferences and then sends pop-ups and ads to the user that match their tastes. A virus is a program that attempts to damage a computer system and replicate itself to other computer systems. A Trojan horse is a malicious program that is disguised as legitimate software.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_06]

▼ Question 5: Correct

What is a cookie?

○ A malicious program that runs when you read an email attachment.

○ A malicious program that disguises itself as a useful program.

➡ ● A file saved on your hard drive that tracks website preferences and use.

○ An executable file that runs in the background and tracks internet use.

Explanation

A cookie is a file saved on your hard drive that tracks website preferences and use. Many legitimate websites use cookies to remember your preferences and make the websites easier to use. However, other sites can use cookies to track personal information.

Spyware is a program that runs in the background and reports internet use to servers on the internet. A Trojan horse is a malicious program that disguises itself as a useful program. Programs do not run when you simply read an email attachment. However, many malicious script programs are disguised as simple text files and can cause damage if you run the script file.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_07]

▼ Question 6: Correct

Which type of malicious activity can be described as numerous unwanted and

➡ ● Spamming

○ Crimeware

○ Trojan

○ Email hijacking

Explanation

Spamming is a type of malicious activity in which numerous unwanted and unsolicited email messages are sent to a wide range of victims. Spam itself may or may not be malicious in nature. Unfortunately, spam accounts for 40 to 60 percent of the email traffic on the internet. Most of this activity is unsolicited.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_08]

Question 7: Correct

While browsing the internet, you notice that your browser displays pop-ups containing advertisements that are related to recent keyword searches you have performed.

What is this an example of?

➡ ● Adware

○ Trojan

○ Worm

○ Grayware

Explanation

Adware monitors actions that denote personal preferences and then sends pop-ups and ads that match those preferences. Adware is:

- Usually passive.
- Invasive.
- Installed on your machine when you visit a website or run an application.
- Usually more annoying than harmful.

A worm is a self-replicating virus. Grayware is software that might offer a legitimate service, but also includes features that you aren't aware of or features that could be used for malicious purposes. A Trojan horse is a malicious program that is disguised as legitimate or desirable software.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_09]

Question 8: Correct

What is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is

○ Buffer overflow

○ Trojan

➡ ● Virus

○ Password attack

Explanation

A virus is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found. Viruses are a serious threat to computer systems, especially if they are connected to the internet. You should install anti-malware software on every computer in your network to protect against viruses.

Trojan horses are programs that claim to serve a useful purpose, but hide a malicious purpose or activity. A buffer overflow is partially correct in that a buffer overflow may be used as an insertion vector for a virus. A password attack attempts to identify the password used by a user account.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_10]

Question 9: Correct

What are the most common means of virus distribution? (Select TWO).

➡ ☑ Malicious websites

□ Commercial software CDs

□ Floppy disks

□ Downloading music files from the internet

➡ ☑ Email

Explanation

Email is the most common means of virus distribution. Often, viruses will 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. Malicious websites are also frequently used for virus distribution. 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 from your system.

Downloaded music files and commercial software CDs all have the potential to spread viruses, but they are not as commonly employed.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_SEC_SW_11]

Question 10: Incorrect

Which of the following BEST describes what happened to the file?

○ The file extension has been changed to prevent it from running.

➡ ○ It has been moved to a folder on your computer.

○ It has been deleted from your system.

● ~~The infection has been removed, and the file has been saved to a different location.~~

Explanation

Quarantine moves the infected file to a secure folder, where it cannot be opened or run normally. By configuring the software to quarantine any problem files, you can view, scan, and try to repair those files. Quarantine does not automatically repair files. Deleting a file is one possible action to take, but this action removes the file from your system.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_ANTIV_FCT_04]

▼ **Question 11:** Correct

You have a computer that runs Windows 10. Where would you go to verify that the system has recognized the anti-malware software installed on the system?

➡ ● Security and Maintenance

○ Windows Firewall

○ Network and Sharing Center

○ System

Explanation

Use Security and Maintenance in Control Panel to check the current security status of your computer. Security and Maintenance displays whether you have anti-malware, firewall, and automatic updates configured.

Use the firewall to open and close firewall ports. Use System to perform tasks such as viewing system information and enabling Remote Desktop. Use the Network and Sharing Center to view the status of your network connections.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_ANTIV_FCT_07]

▼ **Question 12:** Correct

You have recently had an issue where a user's Windows computer was infected with a virus.

After removing the virus from the computer, which of the following is the NEXT step you should take?

○ Educate the user.

➡ ● Install all OS updates.

○ Enable System Restore.

Explanation

After an infected computer has been remediated successfully, the next step in the best practice procedures for malware removal states that you should ensure that all OS updates are installed and that regular virus scans are scheduled.

Following that action, you should enable system restore, create a new restore point, and educate end users on better practices.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_ANTIV_FCT_09]

▼ **Question 13:** Incorrect

Your anti-malware software has detected a virus on your Windows 10 system. However, the anti-malware software is unable to remove it. When you try to delete the files, you can't because they are in use.

Which of the following actions would be BEST to try first?

○ Run Sfc.exe.

○ Reset the operating system.

➡ ○ Boot into Safe Mode and try removing the malware.

● ~~Update the anti-malware definition files.~~

Explanation

If a malware process is running and you are unable to stop it, try booting into Safe Mode and then run the scanning software to locate and remove the malware (or delete the files manually). Safe Mode loads only the required drivers and processes.

Anti-malware definition files are used to identify a virus; in this case, the anti-malware software has already detected the virus so the files are sufficiently up-to-date to detect the virus. Resetting the operating system might be necessary, but should only be tried after all other measures have failed. Sfc.exe checks and repairs system files.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_ANTIV_FCT_10]

▼ **Question 14:** Incorrect

A user reports that his machine will no longer boot properly. After asking several questions to determine the problem, you suspect the user unknowingly downloaded malware from the internet, and that the malware corrupted the boot block.

Based on your suspicions, which of the following actions would you MOST likely take

☑ ~~Boot into Safe Mode and try removing the malware.~~

➡ ☑ Boot from the Windows installation DVD and use the Recovery Environment to run a startup repair.

□ Have the user attend an internal internet safety training course.

□ Run sfc.exe.

➡ □ Reimage the machine.

Explanation

From the Recovery Environment, run a startup repair operation. If you have an existing image of the computer, you could also reimage the system. However, all data and applications added to the system since the image was created will be lost. Reimaging the system will typically get Windows back up and running on the computer more quickly than manually re-installing the operating system.

User training is a preventative measure against malware infections; however, the training will not repair the current damage. Sfc.exe scans every system file in the operating system for altered files, but does not scan the master boot record or the volume boot record. Since the machine no longer boots properly, booting into Safe Mode is not an option in this scenario.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_ANTIV_FCT_11]

▼ **Question 15:** Correct

Which of the following is the process of fixing problems detected by anti-virus software so that the computer is restored to its original state?

○ Quarantine

○ Scanning

○ Isolation

➡ ● Remediation

Explanation

Remediation is the process of correcting any problems that are found. Most antivirus software remediates problems automatically or semi-automatically (you are prompted to identify the action to take).

Quarantine is the process of moving an infected file or computer to a safe location so that the problem cannot affect or spread to other files or computers. Isolation is one method of performing quarantine. Scanning is the process of checking a system for infected files.

References

TestOut PC Pro - 13.6 Malware Protection
[e_malware_pp6.exam.xml Q_ANTIV_FCT_15]