Exam Report: 7.1.7 Practice Questions

Date: 1/22/2020 1:39:29 pm
Time Spent: 14:51

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

What is the main difference between a worm and a virus?

○ A worm is restricted to one system, while a virus can spread from system to system.

➡ ◉ A worm can replicate itself, while a virus requires a host for distribution.

○ A worm requires an execution mechanism to start, while a virus can start itself.

○ A worm tries to gather information, while a virus tries to destroy data.

Explanation

A *worm* is a self-replicating program that uses the network to replicate itself to other systems. A worm does not require a host system to replicate.

Both viruses and worms can cause damage to data and systems, and both spread from system to system, although a worm can spread itself while a virus attaches itself to a host for distribution.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_01]

Question 2: Correct

A collection of zombie computers have been set up to collect personal information. What type of malware do the zombie computers represent?

➡ ◉ Botnet

○ Logic bomb

○ Trojan horse

○ Spyware

Explanation

A *botnet* is a collection of zombie computers that are commanded from a central control infrastructure and propagate spam or to collect usernames and passwords to access secure information.

A *logic bomb* is malware that lies dormant until triggered. A *Trojan horse* is a malicious program that is disguised as legitimate software. *Spyware* monitors the actions performed on a machine and then sends the information back to its originating source.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_03]

Question 3: Correct

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

➡ ● Trojan horse

○ Worm

○ Outlook Express

○ ActiveX control

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 very common on the internet. 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.

Outlook Express is an email client found on Windows. 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. ActiveX controls are web applications written in the framework of ActiveX.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_04]

▼ **Question 4:** Correct

Which of the following is undetectable software that allows administrator-level access?

○ Spyware

○ Worm

○ Logic bomb

○ Trojan horse

➡ ● Rootkit

Explanation

A *rootkit* is a set of programs that allows attackers to maintain permanent, administrator-level, hidden access to a computer. A rootkit:

- Is almost invisible software
- Resides below regular antivirus software detection
- Requires administrator privileges for installation, then maintains those privileges to allow subsequent access
- Might not be malicious
- Often replaces operating system files with alternate versions that allow hidden access

A *worm* is a self-replicating virus. A *Trojan horse* is a malicious program that is disguised as legitimate or desirable software. A *logic bomb* is designed to execute only under predefined conditions and lays dormant until the predefined condition is met. *Spyware* is software that is installed without the user's consent or knowledge and designed to intercept or take partial control over the user's interaction with the computer.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_07]

▼ **Question 5:** Correct

Which of the following are characteristics of a *rootkit*? (Select two.)

➡ ☑ Hides itself from detection

□ Uses cookies saved on the hard drive to track user preferences

➡ ☑ Requires administrator-level privileges for installation

□ Monitors user actions and opens pop-ups based on user preferences

Explanation

A *rootkit* is a set of programs that allows attackers to maintain hidden, permanent, administrator-level access to a computer. A rootkit:

- Is almost invisible software
- Resides below regular antivirus software detection
- Requires administrator privileges for installation, then maintains those privileges to allow subsequent access
- Might not be malicious
- Often replaces operating system files with alternate versions that allow hidden access

Spyware collects various types of personal information, such as internet surfing habits and passwords, and sends the information back to its originating source. *Adware* monitors actions that denote personal preferences, then sends pop-ups and ads that match those preferences. Both Spyware and adware can use cookies to collect and report a user's activities.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_08]

Question 6: Incorrect

You have heard about a new malware program that presents itself to users as a virus scanner. When users run the software, it installs itself as a hidden program that has administrator access to various operating system components. The program then tracks system activity and allows an attacker to remotely gain administrator access to the computer.

Which of the following terms best describes this software?

➡ ○ Rootkit

○ Botnet

○ Privilege escalation

○ Trojan horse

● ~~Spyware~~

Explanation

This program is an example of a rootkit. A *rootkit* is a set of programs that allow attackers to maintain permanent, administrator-level, and hidden access to a computer. Rootkits require administrator access for installation and typically gain this access using a Trojan horse approach--masquerading as a legitimate program to entice users to install the software.

While this program is an example of a Trojan horse that also performs spying activities (spyware), the ability to hide itself and maintain administrator access makes *rootkit* a better description for the software. A botnet is a group of zombie computers that are commanded from a central control infrastructure.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_09]

Question 7: Correct

Which of the following best describes *spyware*?

○ It is a malicious program disguised as legitimate software.

- ➡ ● It monitors the actions you take on your machine and sends the information back to its originating source.
- ○ It is a program that attempts to damage a computer system and replicate itself to other computer systems.
- ○ It monitors user actions that denote personal preferences, then sends pop-ups and ads to the user that match their tastes.

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 denote their personal preferences, 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 disguised as legitimate software.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_11]

Question 8: Correct

What is the primary distinguishing characteristic between a worm and a logic bomb?

- ○ Incidental damage to resources
- ➡ ● Self-replication
- ○ Masquerades as a useful program
- ○ Spreads via email

Explanation

The primary distinguishing characteristic between a worm and a logic bomb is self-replication. Worms are designed to replicate and spread as quickly and as broadly as possible. Logic bombs do not self-replicate. They are designed for a specific single system or type of system. Once planted on a system, it remains there until it is triggered.

Both worms and logic bombs can be spread via email, and both may cause incidental damage to resources. While either may be brought into a system as a parasite on a legitimate program or file or as the payload of a Trojan horse, the worm or logic bomb itself does not masquerade as a useful program.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_13]

Question 9: Correct

What is another name for a logic bomb?

- ○ DNS poisoning
- ➡ ● Asynchronous attack
- ○ Trojan horse
- ○ Pseudo flaw

Explanation

A logic bomb is a specific example of an asynchronous attack. An asynchronous attack is a form of malicious attack where actions taken at one time do not cause their intended, albeit negative, action until a later time.

A pseudo flaw is a form of IDS that detects when an intruder attempts to perform a common but potentially dangerous administrative task. DNS poisoning is the act of inserting incorrect domain name or IP address mapping information into a DNS server or a client's cache. A Trojan horse is any malicious code embedded inside of a seemingly benign carrier. None of these three terms is a synonym for logic bomb.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_14]

▼ **Question 10:** Incorrect

You have installed anti-malware software that checks for viruses in email attachments. You configure the software to quarantine any files with problems.

You receive an email with an important attachment, but the attachment is not there. Instead, you see a message that the file has been quarantined by the anti-malware software.

What has happened to the file?

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

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

○ It has been deleted from your system.

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

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 possibly 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

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_15]

▼ **Question 11:** Correct

Which of the following statements about the use of anti-virus software is correct?

○ Once installed, anti-virus software needs to be updated on a monthly basis.

➡ ● Anti-virus software should be configured to download updated virus definition files as soon as they become available.

○ If servers on a network have anti-virus software installed, workstations do not need anti-virus software installed.

○ If you install anti-virus software, you no longer need a firewall on your network.

Explanation

Anti-virus software is only effective against new viruses if it has the latest virus definition files installed. You should configure your anti-virus software to automatically download updated virus definition files as soon as they become available.

Anti-virus software needs to be updated with virus definitions files as soon as they become available, not on a monthly basis. All systems on a network, regardless of whether they are workstations or servers, should have anti-virus software installed on them. An anti-virus solution is not a substitute for a firewall. Firewalls examine network traffic to prevent network-based attacks.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_17]

Question 12: Correct

If your anti-virus software does not detect and remove a virus, what should you try first?

○ Scan the computer using another virus detection program.

➡ ● Update your virus detection software.

○ Search for and delete the file you believe to be infected.

○ Set the read-only attribute of the file you believe to be infected.

Explanation

Virus detection software can search only for viruses listed in its known viruses data file. An outdated file can prevent the virus detection software from recognizing a new virus.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_18]

Question 13: Correct

You have installed anti-virus software on the computers on your network. You update the definition and engine files and configure the software to update those files every day.

What else should you do to protect your systems from malware? (Select two.)

□ Disable UAC

□ Enable account lockout

➡ ☑ Educate users about malware

➡ ☑ Schedule regular full system scans

□ Enable chassis intrusion detection

Explanation

You should schedule regular full system scans to look for any malware. In addition, educate users about the dangers of downloading software and the importance of anti-malware protections.

You should enable User Account Control (UAC) to prevent unauthorized administrative changes to your system. Use Account Lockout to help protect your system from hackers trying to guess passwords. Use chassis intrusion detection to identify when the system case has been opened.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_19]

Question 14: Correct

To tightly control the anti-malware settings on your computer, you elect to update the signature file manually. Even though you vigilantly update the signature file, the machine becomes infected with a new type of malware.

Which of the following actions would best prevent this scenario from occurring again?

○ Create a scheduled task to run **sfc.exe** daily

○ Carefully review open firewall ports and close any unnecessary ports

➡ ● Configure the software to automatically download the virus definition files as soon as they become available

○ Switch to a more reliable anti-virus software

Explanation

Anti-malware software is most effective against new viruses if it has the latest virus definition files installed. Instead of manually updating the signature files, you should configure the software to automatically download updated virus definition files as soon as they become available.

Use **sfc.exe** to repair infected files after malware has caused the damage. Using a different anti-virus software might help, but will not resolve the problem if you don't get the latest definition files.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_20]

▼ **Question 15:** Incorrect

Which type of virus conceals its presence by intercepting system requests and altering service outputs?

○ Retro

● ~~Polymorphic~~

○ Slow

➡ ○ Stealth

Explanation

Stealth viruses reside in low-level system service functions where they intercept system requests and alter service outputs to conceal their presence. The term *rootkit* is often used to describe a malicious program that can hide itself and prevent its removal from the system.

A *polymorphic* virus mutates while keeping the original algorithm intact. A *slow* virus counters the ability of antivirus programs to detect changes in infected files. A *retro* virus tries to destroy virus countermeasures by deleting key files that antivirus programs use.

References

LabSim for Security Pro, Section 7.1.
[All Questions SecPro2017_v6.exm MALWARE_22]