Exam Report: 13.13.4 Practice Questions

Date: 4/15/2020 5:43:11 pm
Time Spent: 2:17

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 70%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Alice has received several calls from her friends informing her that they are receiving strange emails containing content that seems odd coming from her.

Which of the following MOST likely happened on Alice's computer?

➡ ● Alice's email account was hijacked.

○ A family member used her account to send prank emails.

○ A virus or malware was installed on Alice's computer.

○ A Trojan horse is running on Alice's computer.

Explanation

Although a family member may have tried to play a trick on Alice, it is more plausible that her email was hijacked. Hijacked or hacked email accounts are suspected when those receiving the emails are confused by or suspicious of the email's content. Another indication of a hijacked email account is automated replies from unknown sent email.

Email accounts can be hijacked using several techniques. Therefore, it may or may not be caused by malware or a Trojan horse. For example, some email providers, such as Yahoo, can have their systems compromised, and your email information (username and password) are sold and used to access your account. Since it is also possible that your email was compromised through malicious software, you should take the proper steps to verify that all malware software is removed.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_COMM_NETATT_01]

Question 2: Correct

A user within your organization received an email relating how an account containing a large sum of money has been frozen by the government of a small middle eastern nation. The user was offered a 25% share of this account if she would help the sender transfer it to a bank in the United States. The user responded and was instructed to wire $5,000 to the sender to facilitate the transfer. She complied, but has not heard

Which of the following BEST describes the type of attack which as occurred in this scenario?

- ○ Eavesdropping
- ○ Man-in-the-middle
- ➡ ● Nigerian 419 scam
- ○ Vishing

Explanation

A phishing attack has occurred in this scenario. This particular attack is sometimes referred to as a Nigerian 419 scam, and is very common.

Vishing is similar to phishing, but instead of an email, the attacker uses Voice over IP (VoIP) to gain sensitive information. Eavesdropping refers to an unauthorized person listening to conversations of employees or other authorized personnel discussing sensitive topics. A man-in-the-middle attack is a technological attack where a malicious person intercepts network communications between two hosts, posing as the sender to the receiver and as the receiver to the sender.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_COMM_NETATT_02]

▼ **Question 3:** Correct

Which of the following describes a man-in-the-middle attack?

- ○ A person over the phone convinces an employee to reveal their logon credentials.
- ➡ ● An attacker intercepts communications between two network hosts by impersonating each host.
- ○ An IP packet is constructed which is larger than the valid size.
- ○ Malicious code is planted on a system where it waits for a triggering event before activating.

Explanation

A man-in-the-middle attack is a technological attack where a malicious person intercepts network communications between two hosts, posing as the sender to the receiver and as the receiver to the sender.

Convincing an employee over the phone to reveal his logon credentials is an example of a social engineering attack. Constructing an IP packet which is larger than the valid size is a form of denial of service attack. Planting malicious code on a system where it waits for a triggering event before activating is a logic bomb.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_COMM_NETATT_03]

▼ **Question 4:** Incorrect

Which of the following BEST describes the type of attack which as occurred in this scenario?

- ○ Sniffing
- ● ~~Session hijacking~~
- ○ Man-in-the-middle
- ○ Snooping
- ➡ ○ Spoofing

Explanation

This is an example of spoofing. Spoofing involves changing or falsifying information in order to mislead or re-direct traffic. In this scenario, the router's external interface cannot receive a valid packet with a source address from the internal network. One must assume that the source address of the packet was faked.

Snooping is the act of spying into private information or communications. One type of snooping is sniffing. Sniffing is the act of capturing network packets in order to examine the contents of communications. A man-in-the-middle attack is a technological attack where a malicious person intercepts network communications between two hosts, posing as the sender to the receiver and as the receiver to the sender. Session hijacking is an extension of a man-in-the-middle attack where the attacker hijacks an active communication session.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_COMM_NETATT_04]

▼ **Question 5:** Correct

The TCP/IP session state between two computers on a network is being manipulated by an attacker such that she is able to insert tampered packets into the communication stream.

Which of the following BEST describes the type of attack which as occurred in this scenario?

- ○ Spear phishing
- ○ Whaling
- ○ Phishing
- ➡ ● Hijacking

Explanation

A hijacking attack has occurred. Hijacking happens when the TCP/IP session state is manipulated such that a third party is able to insert alternate packets into the communication stream.

A phishing scam employs an email pretending to be from a trusted organization, asking to verify personal information or send a credit card number. In spear

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_COMM_NETATT_05]

▼ **Question 6:** Correct

While browsing the internet, a pop-up browser window is displayed warning you that your system is infected with a virus. You are directed to click a link to remove the virus.

Which of the following are the next BEST actions to take? (Select TWO).

☐ Use a search engine on the Internet to learn how to manually remove the virus.

☐ Click on the link provided to scan for and remove the virus.

➡ ☑ Run a full system scan using the anti-malware software installed on your system.

☐ Close the pop-up window and ignore the warning.

➡ ☑ Update the virus definitions for your locally-installed anti-malware software.

Explanation

This is an example of a rogue anti-virus attack. As such, you should assume that your system may have been infected by some time of malware, possibly by one of the sites you visited recently.

You should first close your browser window and then update the virus definitions for your locally-installed anti-virus software. Once done, you should Run a full system scan using the anti-virus software installed on your system.

Clicking the link provided would be the worst choice as it will most likely install a host of malware on your system. Ignoring the message is unwise as your system has probably been infected with malware that should be removed. You shouldn't try to manually remove the virus as the message displayed by the rogue anti-virus attack is probably fictitious.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_SEC_ISSUES_01]

▼ **Question 7:** Incorrect

Which of the following techniques are used in a pharming attack to redirect legitimate web traffic to malicious websites? (Select TWO).

☐ Dictionary attack

☐ Search engine results poisoning

➡ ☐ Changing the hosts file of a user's computer

➡ ☑ Exploiting DHCP servers to deliver the IP address of poisoned DNS servers

Explanation

Pharming redirects one website's traffic to a bogus website designed to look like the real website. Once the user is there, the attacker tricks the user into supplying personal information, such as bank account and PIN numbers. Pharming works by resolving legitimate URLs to the IP address of malicious websites. This is typically done using one of the following techniques:

- Changing the hosts file of a user's computer
- Poisoning a DNS server
- Exploiting DHCP servers to deliver the IP address of malicious DNS servers in DHCP leases

Search engine results poisoning is not typically associated with pharming attacks. A man-in-the-middle attack occurs when the attacker intercepts legitimate network traffic and then poses as one of the parties involved in the network communication. A dictionary attack is used to crack passwords by guessing the password from a list of likely words.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_SEC_ISSUES_02]

▼ **Question 8:** Correct

Which of the following are likely symptoms of malware infection? (Select TWO).

☐ Operating system updates that were installed without your knowledge

➡ ☑ Renamed system files

☐ Receipt of phishing emails in your inbox

➡ ☑ Changed file permissions

☐ Cookies placed by a website recently visited

Explanation

Common symptoms of a malware infection include the following:

- Slow computer performance
- Internet connectivity issues
- Operating system lock ups
- Windows update failures
- Renamed system files
- Disappearing files
- Changed file permissions
- Access denied errors

Cookies are commonly placed by legitimate websites and aren't considered a major security threat. Windows operating systems automatically install updates by default. Receiving phishing emails doesn't necessarily indicate that the system is infected with malware. It's more likely your email address has been picked up and included on a list.

References

[e_sectrb_pp6.exam.xml Q_SEC_ISSUES_03]

▼ **Question 9:** Incorrect

Some software on Rachel's computer is telling her that her computer is at risk and that she needs to purchase an upgrade for the software before the risk can be removed. Confused, Rachel calls you (the IT specialist) for advice.

After meeting with Rachel, you discover that the pop-up warnings only began after she installed a plug-in for her internet browser.

Which of the following is the MOST likely cause of these warning messages?

○ Hijacked email

➡ ○ Rogue antivirus

○ App scanner

● ~~SPAM~~

Explanation

Rogue antiviruses are programs maliciously added to a computer, which will then often display pop-up or warning messages that try to scare a user into purchasing fake products to clean their computers.

SPAM is the type of unwanted and unsolicited email a user gets. Hijacked email is when someone deceptively takes over your legitimate email account, typically by guessing your password. App scanner is software that allows a mobile phone to scan documents.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_SEC_ISSUES_04]

▼ **Question 10:** Correct

You are an IT technician for your company. Vivian has been receiving error messages indicating that some of her Windows system files are corrupt or missing. To fix this issue, you ran the Windows System File Checker tool (SFC.exe).

Shortly after the files were repaired, Vivian calls again because she is still having the same issue. You now suspect that the corruption or renaming of the system files is being caused by malware.

Which of the following is the next BEST step that should be taken?

○ Disable System Restore.

➡ ● Quarantine Vivian's computer.

○ Perform a scan using anti-malware software.

○ Back up Vivian's critical files and perform a clean install of Windows.

Explanation

When you suspect that a computer may be infected with malware, you should

Backing up an infected computer only saves the problem for future users.

References

TestOut PC Pro - 13.13 Security Troubleshooting
[e_sectrb_pp6.exam.xml Q_SEC_ISSUES_05]