Exam Report: 13.3.9 Practice Questions

Date: 12/2/2019 10:28:04 am
Time Spent: 11:33

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

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

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

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, 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 prevent outside users from gaining access to the network. They do not protect the network from viruses.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm NP05_3-10 #24]

Question 2: Correct

An attacker sets up 100 drone computers that flood a DNS server with invalid requests. This is an example of which kind of attack?

- Spamming
- DoS
- Replay
- DDoS
- Backdoor

Explanation

A DDoS attack is when multiple PCs attack a victim simultaneously and generate excessive traffic that overloads communication channels or exploiting software flaws.

A DoS attack is when a single attacker directs an attack at a single target. Spamming is just a traffic generation form of attack where unrequested messages are sent to a victim. Replay and backdoor attacks are both just flaw exploitation attacks. Replay attacks exploit software flaws by capturing traffic, editing it, then replaying the traffic in an attempt to gain access to a system. Backdoor attacks exploit software flaws by obtaining access codes or account credentials to bypass security. Backdoors can also be planted by hackers to allow easy re-access to a compromised system.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm SSCP-4 [536]]

Question 3: Incorrect

Which of the following is a form of denial of service attack that uses spoofed ICMP packets to flood a victim with echo requests using a bounce/amplification network?

- Smurf
- Fraggle
- ~~Session hijacking~~
- Fingerprinting

Explanation

Smurf is a form of denial of service attack that uses spoofed ICMP packets to flood a victim with echo requests using a bounce/amplification network.

Fingerprinting is the act of identifying an operating system or network service based on its ICMP message quoting characteristics. A fraggle attack uses spoofed UDP packets to flood a victim with echo requests using a bounce network, similar to a Smurf attack. Session hijacking is the act of taking over a logon session from a legitimate client, impersonating the user and taking advantage of their established communication link.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm SSCP-4 [568]]

Question 4: Correct

An attacker captures packets as they travel from one host to another with the intent of altering the contents of the packets. Which type of attack is being executed?

- Passive logging
- Spamming
- Man-in-the-middle attack
- Distributed denial of service

Explanation

Capturing packets between two existing communication partners is a form of man-in-the middle attack. This attack's name comes from the way traffic is intercepted somewhere between or in the middle of the two communicating partners. The best way to protect a system from man-in-the middle attacks is to use session encryption or line encryption solutions.

Passive logging is a means of recording information about network traffic or operations in a system without affecting either in any way.

References

LabSim for Network Pro, Section 13.3.

[netpro18v5_all_questions_en.exm SSCP-4 SP [376]]

Question 5: Correct

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

- Outlook Express
- Worm
- Trojan horse
- ActiveX controls

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 whose primary purpose is to duplicate itself and spread, but does not necessarily intentionally damaging or destroying resources. ActiveX controls are web applications written in the framework of ActiveX.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm SSCP-4 SP [238]]

Question 6: Correct

Which type of activity changes or falsifies information in order to mislead or re-direct traffic?

- Snooping
- Sniffing
- Spoofing
- Spamming

Explanation

Spoofing changes or falsifies information in order to mislead or re-direct traffic.

Snooping is the act of spying into private information or communications. One type of snooping is sniffing. Sniffing captures network packets in order to examine the contents of communications. Spamming is sending a victim unwanted and unrequested email messages.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm SSCP-4 SP [416]]

Question 7: Incorrect

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?

- ~~Phishing~~
- Spam
- Repudiation attack

- ◯ Open SMTP relay

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, containing phishing attacks, 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 Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm MCS1]

Question 8: Correct

An attacker uses an exploit to push a modified hosts file to client systems. This hosts file redirects traffic from legitimate tax preparation sites to malicious sites to gather personal and financial information.

What kind of exploit has been used in this scenario? (Select two. Both responses are different names for the same exploit.)

- ☐ Reconnaissance
- ➡ ☑ DNS poisoning
- ➡ ☑ Pharming
- ☐ Domain name kiting
- ☐ Man-in-the-middle

Explanation

DNS poisoning (also known as DNS cache poisoning or Pharming) occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses.

In a DNS poisoning attack:

- Incorrect DNS data is introduced into the cache of a primary DNS server.
- The incorrect mapping is made available to client applications.
- Traffic is redirected to incorrect sites for phishing purposes.

Reconnaissance is used to gather information for an attack. The goal is to obtain DNS records that identify computer names and IP addresses in a network. Domain name kiting occurs when spammers exploit domain registration by taking advantage of the five-day grace period for a newly registered domain name to acquire domains and never pay for their registration. Attackers accomplish this task by unregistering a domain name just before the grace period is up and then immediately re-registering the domain name. Man-in-the-middle attacks are used to intercept information passing between two communication partners.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm MCM1||/]

Question 9: Incorrect

A programmer that fails to check the length of input before processing, leaves his code vulnerable to what form of common attack?

- ~~Session hijacking~~
- Buffer overflow
- Backdoor
- Privilege escalation

Explanation

Buffer overflow attacks are made possible by oversight on the part of the programmers. A simple check on the length (and sometimes format) of input data before processing eliminates buffer attacks.

A backdoor is a developer-planted or cracker-planted entry device that bypasses security to gain access to a system or software. A developer-planted backdoor is often a debugging tool that was mistakenly left in place when the software went to market. A cracker-planted device is often a remote access server that listens for inbound connections on a specific port. Either method can be used by an intruder to gain entry into a secured environment.

Session hijacking is the concept of being able to take over a communication session between a client and server. This usually involves taking over the identity of the client and fooling the server into communicating with the pseudo client. Privilege escalation is when a user steals or otherwise obtains high-level privileges in a computer system.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm SSCP-4 SP [632]||/]

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?

- The file extension has been changed to prevent it from running.
- It has been deleted from your system.
- ~~The infection has been removed, and the file has been saved to a different location.~~
- It has been moved to a secure folder on your computer.

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 Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm AP09PA_4-1 D5]

Question 11: Correct

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

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

- [x] Update your virus detection software.
- [ ] Scan the computer using another virus detection program.
- [ ] 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 Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm APESS_6-4 [7]]

Question 12: Correct

Which of the following measures are you most likely to implement to protect a system from a worm or Trojan horse?

- [x] Antivirus software
- [ ] Firewall
- [ ] IPsec
- [ ] Password policy

Explanation

Worms and Trojan horses are types of viruses. The best way to protect a system from them is to ensure that every system on the network has antivirus software with up-to-date virus definitions installed.

A firewall helps prevent hackers from penetrating a network from the internet. They do not specifically guard against viruses, though some application-level firewall solutions do include antivirus capabilities. IPsec is an encryption mechanism. A password policy enforces password composition rules and helps prevent authentication attacks.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm APESS_6-1 [66]]

Question 13: 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?

- [ ] Carefully review open firewall ports and close any unneeded ports.
- [x] Configure the software to automatically download the virus definition files as soon as they become available.
- [ ] Switch to a more reliable anti-virus software.
- [ ] Create a scheduled task to run **sfc.exe** daily.

Explanation

Anti-malware software is most effective 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 Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm AP09PA-4-1 #3]

Question 14: Incorrect

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.)

- [x] Educate users about malware.
- [ ] Enable chassis intrusion detection.
- [x] ~~Enable account lockout.~~
- [x] Schedule regular full system scans.
- [ ] Disable UAC.

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 Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm AP09PA-4-1 D8]

Question 15: Correct

While using the internet, you type the URL of one of your favorite sites in the browser. Instead of going to the correct site, the browser displays a completely different website. When you use the IP address of the web server, the correct site is displayed.

Which type of attack has likely occurred?

- ( ) Spoofing
- (•) DNS poisoning
- ( ) Hijacking
- ( ) Man-in-the-middle

Explanation

Because the correct site shows when you use the IP address, you know that the main website is still functional and that the problem is likely caused by an incorrect domain name mapping. DNS poisoning occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. In a DNS poisoning attack:

- Incorrect DNS data is introduced into the cache of a primary DNS server.
- The incorrect mapping is made available to client applications through the resolver.

Spoofing is used to hide the true source of packets or redirect traffic to another location. Spoofing attacks use modified source and/or destination addresses in packets and can include site spoofing that tricks users into revealing information. A man-in-the-middle attack is used to

intercept information passing between two communication partners. TCP/IP hijacking is an extension of a man-in-the-middle attack where the attacker steals an open and active communication session from a legitimate user. In spoofing, man-in-the-middle, and hijacking attacks, the attack would be successful regardless of whether the DNS name or the IP address were used.

References

LabSim for Network Pro, Section 13.3.
[netpro18v5_all_questions_en.exm SP08_2-1 2]