Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE 100%

Understanding Security Threats

LATEST SUBMISSION GRADE
100%

1. Question — 1 / 1 point

Phishing, baiting, and tailgating are examples of _____ attacks.

- Password
- Network
- Social engineering
- Malware

Correct
Yep! These three attack types are designed to trick or deceive people into trusting an attacker. Phishing accomplishes this via email, baiting uses physical props like USB drives, and tailgating happens when the attacker follows you into a restricted area.

2. Question — 1 / 1 point

When cleaning up a system after a compromise, you should look closely for any _____ that may have been installed by the attacker.

- Rogue APs
- Injection attacks
- Backdoors
- Poisoned DNS caches

Correct
Woohoo! Attackers commonly install backdoors in systems that they compromise to maintain access to the system even after the vulnerability they exploited originally gets patched.

3. Question — 1 / 1 point

A SYN flood occurs when the attacker overwhelms a server with _____.

- SYN packets
- Injection attacks
- Malware
- ACK packets

Correct
Nice work! A SYN flood attack happens when the attacker floods the victim with SYN packets and never completes the TCP three-way handshake.

4. Question — 1 / 1 point

The best defense against injection attacks is to _____.

- Use input validation
- Use antimalware software
- Use strong passwords
- Use a firewall

Correct
You nailed it! Input validation will prevent an attacker from injecting commands using text input fields.

5. Question — 1 / 1 point

Which of these is an example of the confidentiality principle that can help keep your data hidden from unwanted eyes?

- Protecting online accounts with password protection
- Preventing data loss
- Preventing an unwanted download
- Making sure the data hasn't been tampered with

Correct
Nice job! Password protection can help limit access to your data so that only those who need it can see it.

6. Question — 1 / 1 point

What could potentially decrease the availability of security and also test the preparedness of data loss?

- Ransomware
- Keylogger
- Adware
- Spyware

Correct
Great work! Ransomware could prevent access to your data by holding the data hostage until you pay a ransom.

7. Question — 1 / 1 point

What's the difference between a virus and a worm?

- Viruses do not replicate like worms do.
- Worms replicate; viruses do not.
- Worms replicate through files, but viruses live on their own.
- Viruses replicate through files, but worms live on their own.

Correct
Woohoo! Viruses and worms are similar. The difference is that a virus spreads through files and worms don't need to attach to something to spread.

8. Question — 1 / 1 point

What is it called when a hacker is able to get into a system through a secret entryway in order to maintain remote access to the computer?

- A Trojan
- A backdoor
- Ransomware
- Adware

Correct
You nailed it! A backdoor is a way for a hacker to get into a system through a secret entryway.

9. Question — 1 / 1 point

A hacker stood outside a building and spun up a wireless network without anyone's knowledge. At that point, the hacker was able to gain unauthorized access to a secure corporate network. Which of these is the name of this type of attack?

- A Denial-of-Service (DoS) attack
- A DNS Cache Poisoning attack
- SYN flood attack
- A Rogue AP (Access Point) attack

Correct
Nice job! A Rogue AP is an access point that is installed on the network without the network admin's knowledge. This is very dangerous because this can allow a hacker to gain unauthorized access to a secure network.

10. Question — 1 / 1 point

What can occur during a ping of death (POD) attack? Check all that apply.

- [x] A Denial-of-Service (DoS)
  - Correct: Right on! A POD is a type of DoS attack.
- [x] A buffer overflow
  - Correct: Woohoo! A POD can result in a buffer overflow.
- [ ] Baiting
- [x] Remote code execution
  - Correct: Woohoo! A POD can result in a buffer overflow which allows for the remote execution of malicious code.

Correct
Great, you got all the right answers.

11. Question — 1 / 1 point

How can injection attacks be prevented? Check all that apply.

- [x] Data sanitization
  - Correct: Well done! Injection attacks can be mitigated with good software development principles such as sanitizing data.
- [x] Input validation
  - Correct: Well done! Injection attacks can be mitigated with good software development principles such as validating input.
- [ ] Flood guards
- [ ] Log analysis systems

Correct
Great, you got all the right answers.

12. Question — 1 / 1 point

Which of these is a way to help prevent brute-force attacks? Check all that apply.

- [x] Strong passwords
  - Correct: You nailed it! The best way to prevent a password attack, such as a brute-force attack, is to utilize strong passwords.
- [ ] Using a precompiled list of common passwords
- [x] Captchas
  - Correct: You nailed it! In a password attack, an automated password cracker could just keep trying to log in to your account, but a captcha prevents these attacks from executing.
- [ ] Password crackers

Correct
Great, you got all the right answers.

13. Question — 1 / 1 point

You receive a legitimate-looking email from a sender that you recognize asking you to click a funny link. But, once you do, malware installs on your computer. What is most likely the reason you got infected?

- The sender's email password was used in a DNS Cache Poisoning attack.
- The sender's email address was spoofed.
- The sender's email password was cracked.
- The sender's email has been hacked.

Correct
You nailed it! It is very easy to send an email and have the From field come from any address you want it to whether it exists or not. For example, you open an email stating it is from your friend's email address that asks you to click a funny link. To you, that seems like a legitimate email, but when you open the link, you suddenly get malware installed. In this case, an attacker spoofed the sender's email address!