COMP3052 Computer Security

Session 04: Authentication

Videoclip: This is How Hackers Crack Passwords!

https://www.youtube.com/watch?v=YiRPt4vrSSw

Videoclip: Brute Force Password Cracking with Hashcat

https://www.youtube.com/watch?v=flU_8pxNQ3g

Videoclip: how to HACK a password // password cracking with Kali Linux and HashCat

https://www.youtube.com/watch?v=z4_oqTZJqCo

1. (Spoofing / Phishing) An email asking the user to confirm personal information – for example, ‘we couldn’t verify your information – click on the link to confirm the same’.

2. (Spoofing / Phishing) Hackers break into a website and change the IP address of the site.

3. (Spoofing / Phishing) Phone calls or emails from your bank requesting an OTP or your bank PIN.

Reference: Phishing vs Spoofing

https://www.educba.com/phishing-vs-spoofing/

4. (Spoofing / Phishing) An email indicating that an Amazon payment had failed.

5. (Spoofing / Phishing) When the user login into a website that appears to be a banking website, the user discovers that the user's account has been stolen.

6. (Spoofing / Phishing) An email that encourages the user with the promise of tax refunds.

Reference: Phishing vs Spoofing

https://www.educba.com/phishing-vs-spoofing/

1. (Spoofing / Phishing) An email asking the user to confirm personal information – for example, ‘we couldn’t verify your information – click on the link to confirm the same’.

2. (Spoofing / Phishing) Hackers break into a website and change the IP address of the site.

3. (Spoofing / Phishing) Phone calls or emails from your bank requesting an OTP or your bank PIN.

Reference: Phishing vs Spoofing

https://www.educba.com/phishing-vs-spoofing/

4. (Spoofing / Phishing) An email indicating that an Amazon payment had failed.

5. (Spoofing / Phishing) When the user login into a website that appears to be a banking website, the user discovers that the user's account has been stolen.

6. (Spoofing / Phishing) An email that encourages the user with the promise of tax refunds.

Reference: Phishing vs Spoofing

https://www.educba.com/phishing-vs-spoofing/

1. What is the term used when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source?

(A) Keylogging
(B) Spoofing
(C) Phishing
(D) Trojan

2. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?

(A) Anonymous Keylogging
(B) Social Engineering
(C) DDoS
(D) Spamming

Reference: Module 2: Quiz – Network Threats (Answers) Network Security

https://itexamanswers.net/module-2-quiz-network-threats-answers-network-security.html

1. What is the term used when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source?

(A) Keylogging

(B) Spoofing

(C) Phishing

(D) Trojan

2. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?

(A) Anonymous Keylogging

(B) Social Engineering

(C) DDoS

(D) Spamming

Reference: Module 2: Quiz – Network Threats (Answers) Network Security

https://itexamanswers.net/module-2-quiz-network-threats-answers-network-security.html

3. What is keylogging?

(A) The act of recording a user's computer screen.

(B) It is when keystrokes do not register correctly on a computer.

(C) The act of recording which keys a user presses on their keyboard.

(D) It is when a malicious actor hacks into someone's social media accounts.

4. Which statement regarding a keylogger is NOT true?

(A) Software keyloggers can be designed to send captured information automatically back to the attacker through the Internet.

(B) Software keyloggers are generally easy to detect.

(C) Hardware keyloggers are installed between the keyboard connector and computer keyboard USB port.

(D) Keyloggers can be used to capture passwords, credit card numbers, or personal information.

Reference: Quesba

https://www.quesba.com/questions/statement-regarding-keylogger-not-true-software-keyloggers-designed-send-823751

3. What is keylogging?

(A) The act of recording a user's computer screen.

(B) It is when keystrokes do not register correctly on a computer.

(C) The act of recording which keys a user presses on their keyboard.

(D) It is when a malicious actor hacks into someone's social media accounts.

4. Which statement regarding a keylogger is NOT true?

(A) Software keyloggers can be designed to send captured information automatically back to the attacker through the Internet.

(B) Software keyloggers are generally easy to detect.

(C) Hardware keyloggers are installed between the keyboard connector and computer keyboard USB port.

(D) Keyloggers can be used to capture passwords, credit card numbers, or personal information.

Reference: Quesba

https://www.quesba.com/questions/statement-regarding-keylogger-not-true-software-keyloggers-designed-send-823751

5. Technicians are testing the security of an authentication system that uses passwords. When a technician examines the password tables, the technician discovers the passwords are stored as hash values. However, after comparing a simple password hash, the technician then discovers that the values are different from those on other systems. What are two causes of this situation? (Choose two.)

(A) Both systems scramble the passwords before hashing.

(B) The systems use different hashing algorithms.

(C) One system uses hashing and the other uses hashing and salting.

(D) Both systems use MD5.

(E) One system uses symmetrical hashing and the other uses asymmetrical hashing.

6. What is a feature of a cryptographic hash function?

(A) Hashing requires a public and a private key.

(B) The hash function is a one-way mathematical function.

(C) The output has a variable length.

(D) The hash input can be calculated given the output value.

Reference: Cybersecurity Essentials FINAL Quiz Answers Full Questions

https://itexamanswers.net/cybersecurity-essentials-final-quiz-answers-full-questions.html

5. Technicians are testing the security of an authentication system that uses passwords. When a technician examines the password tables, the technician discovers the passwords are stored as hash values. However, after comparing a simple password hash, the technician then discovers that the values are different from those on other systems. What are two causes of this situation? (Choose two.)

(A) Both systems scramble the passwords before hashing.

(B) The systems use different hashing algorithms.

(C) One system uses hashing and the other uses hashing and salting.

(D) Both systems use MD5.

(E) One system uses symmetrical hashing and the other uses asymmetrical hashing.

6. What is a feature of a cryptographic hash function?

(A) Hashing requires a public and a private key.

(B) The hash function is a one-way mathematical function.

(C) The output has a variable length.

(D) The hash input can be calculated given the output value.

Reference: Cybersecurity Essentials FINAL Quiz Answers Full Questions

https://itexamanswers.net/cybersecurity-essentials-final-quiz-answers-full-questions.html

7. A user has created a new program and wants to distribute it to everyone in the company. The user wants to ensure that when the program is downloaded that the program is not changed while in transit. What can the user do to ensure that the program is not changed when downloaded?

(A) Create a hash of the program file that can be used to verify the integrity of the file after it is downloaded.

(B) Turn off antivirus on all the computers.

(C) Distribute the program on a thumb drive.

(D) Encrypt the program and require a password after it is downloaded.

(E) Install the program on individual computers.

8. Alice and Bob use the same password to login into the company network. This means both would have the exact same hash for their passwords. What could be implemented to prevent both password hashes from being the same?

(A) Peppering

(B) Pseudo-random generator

(C) Salting

(D) RSA

Reference: Cybersecurity Essentials Chapter 5 Quiz Questions Answers

https://itexamanswers.net/cybersecurity-essentials-chapter-5-quiz-questions-answers.html

7. A user has created a new program and wants to distribute it to everyone in the company. The user wants to ensure that when the program is downloaded that the program is not changed while in transit. What can the user do to ensure that the program is not changed when downloaded?

(A) Create a hash of the program file that can be used to verify the integrity of the file after it is downloaded.

(B) Turn off antivirus on all the computers.

(C) Distribute the program on a thumb drive.

(D) Encrypt the program and require a password after it is downloaded.

(E) Install the program on individual computers.

8. Alice and Bob use the same password to login into the company network. This means both would have the exact same hash for their passwords. What could be implemented to prevent both password hashes from being the same?

(A) Peppering

(B) Pseudo-random generator

(C) Salting

(D) RSA

Reference: Cybersecurity Essentials Chapter 5 Quiz Questions Answers

https://itexamanswers.net/cybersecurity-essentials-chapter-5-quiz-questions-answers.html

9. Which method tries all possible passwords until a match is found?

(A) Brute force

(B) Rainbow tables

(C) Dictionary

(D) Cryptographic

10. A user is evaluating the security infrastructure of a company and notices that some authentication systems are not using best practices when it comes to storing passwords. The user is able to crack passwords very fast and access sensitive data. The user wants to present a recommendation to the company on the proper implementation of salting to avoid password cracking techniques. What are three best practices in implementing salting? (Choose two.)

(A) A salt should not be reused.

(B) A salt should be unique for each password.

(C) The same salt should be used for each password.

(D) Salts should be short.

Reference: Cybersecurity Essentials Chapter 5 Quiz Questions Answers

https://itexamanswers.net/cybersecurity-essentials-chapter-5-quiz-questions-answers.html

9. Which method tries all possible passwords until a match is found?

(A) Brute force

(B) Rainbow tables

(C) Dictionary

(D) Cryptographic

10. A user is evaluating the security infrastructure of a company and notices that some authentication systems are not using best practices when it comes to storing passwords. The user is able to crack passwords very fast and access sensitive data. The user wants to present a recommendation to the company on the proper implementation of salting to avoid password cracking techniques. What are three best practices in implementing salting? (Choose two.)

(A) A salt should not be reused.

(B) A salt should be unique for each password.

(C) The same salt should be used for each password.

(D) Salts should be short.

Reference: Cybersecurity Essentials Chapter 5 Quiz Questions Answers

https://itexamanswers.net/cybersecurity-essentials-chapter-5-quiz-questions-answers.html