Social engineering and malware : *social engineering techniques, indicators of malware-based attacks*

1. What is a common social engineering technique used to trick individuals into disclosing sensitive information?

- A) Phishing

- B) Firewall

- C) Encryption

- D) VPN

- **Answer:** A) Phishing

2. Which of the following is an example of a phishing attack?

- A) Installing antivirus software

- B) Sending an email pretending to be from a bank, asking for login credentials

- C) Using a strong password

- D) Enabling two-factor authentication

- **Answer:** B) Sending an email pretending to be from a bank, asking for login credentials

3. What is the main goal of social engineering attacks?

- A) To install antivirus software

- B) To gain unauthorized access to systems or data

- C) To create strong passwords

- D) To enable two-factor authentication

- **Answer:** B) To gain unauthorized access to systems or data

4. Which of the following is an indicator of a malware-based attack?

- A) Unusual network traffic

- B) Regular software updates

- C) Strong firewall settings

- D) Enabling two-factor authentication

- **Answer:** A) Unusual network traffic

5. What is a common social engineering technique used to manipulate individuals into performing actions or divulging confidential information?

- A) Firewall

- B) Phishing

- C) Encryption

- D) VPN

- **Answer:** B) Phishing

6. Which of the following is an example of pretexting?

- A) A hacker sending a fake email to trick users into providing their login credentials

- B) An attacker posing as an IT support technician and asking for login information

- C) An employee clicking on a malicious link in an email

- D) A company implementing a strong password policy

- **Answer:** B) An attacker posing as an IT support technician and asking for login information

7. What is a common indicator of a malware-based attack?

- A) Regular software updates

- B) Strong firewall settings

- C) Unexpected pop-up windows

- D) Enabling two-factor authentication

- **Answer:** C) Unexpected pop-up windows

8. What is the purpose of a social engineering attack?

- A) To install antivirus software

- B) To gain unauthorized access to information

- C) To create strong passwords

- D) To enable two-factor authentication

- **Answer:** B) To gain unauthorized access to information

9. Which of the following is an example of a social engineering attack?

- A) Installing antivirus software

- B) Using a strong password

- C) Clicking on a malicious link in an email

- D) Enabling two-factor authentication

- **Answer:** C) Clicking on a malicious link in an email

10. What is a common indicator of a malware-based attack?

- A) Unusual network traffic
- B) Regular software updates
- C) Strong firewall settings
- D) Enabling two-factor authentication
- **Answer:** A) Unusual network traffic

11. What is the main goal of a social engineering attack?

- A) To install antivirus software
- B) To gain unauthorized access to systems or data
- C) To create strong passwords
- D) To enable two-factor authentication
- **Answer:** B) To gain unauthorized access to systems or data

12. Which of the following is an example of a pretexting attack?

- A) A hacker sending a fake email to trick users into providing their login credentials
- B) An attacker posing as a bank employee and asking for account information
- C) An employee clicking on a suspicious link in an email
- D) A company implementing a strict password policy
- **Answer:** B) An attacker posing as a bank employee and asking for account information

13. What is a common indicator of a malware-based attack?

- A) Regular software updates

- B) Strong firewall settings

- C) Unexpected system crashes

- D) Enabling two-factor authentication

- **Answer:** C) Unexpected system crashes

14. What is the primary objective of a social engineering attack?

- A) To install antivirus software

- B) To gain unauthorized access to information

- C) To create strong passwords

- D) To enable two-factor authentication

- **Answer:** B) To gain unauthorized access to information

15. Which of the following is an example of a social engineering attack?

- A) Installing antivirus software

- B) Using a strong password

- C) Falling for a scam email and providing personal information

- D) Enabling two-factor authentication

- **Answer:** C) Falling for a scam email and providing personal information

16. What is a common indicator of a malware-based attack?

- A) Unusual network traffic

- B) Regular software updates

- C) Strong firewall settings

- D) Enabling two-factor authentication

- **Answer:** A) Unusual network traffic

17. What is the main objective of a social engineering attack?

- A) To install antivirus software

- B) To gain unauthorized access to systems or data

- C) To create strong passwords

- D) To enable two-factor authentication

- **Answer:** B) To gain unauthorized access to systems or data

18. Which of the following is an example of pretexting?

- A) A hacker sending a fake email to trick users into providing their login credentials

- B) An attacker posing as a customer support representative and asking for account details

- C) An employee clicking on a malicious link in an email

- D) A company implementing a password policy

- **Answer:** B) An attacker posing as a customer support representative and asking for account details

19. What is a common indicator of a malware-based attack?

- A) Regular software updates

- B) Strong firewall settings
- C) Unexpected pop-up windows
- D) Enabling two-factor authentication
- **Answer:** C) Unexpected pop-up windows

20. What is the primary goal of a social engineering attack?

- A) To install antivirus software
- B) To gain unauthorized access to information
- C) To create strong passwords
- D) To enable two-factor authentication
- **Answer:** B) To gain unauthorized access to information

21. Which of the following is an example of a social engineering attack?

- A) Installing antivirus software
- B) Using a strong password
- C) Clicking on a malicious link in an email
- D) Enabling two-factor authentication
- **Answer:** C) Clicking on a malicious link in an email