Test knowledge about hacking

This is a short educational questioning package that aims to give you some techniques that hackers use and help you protect your code from attack. You will be provided with the correct answer with detailed explanation after you have completed all the questions.

This is a short educational questioning package that aims to give you some techniques that hackers use and help you protect your code from attack.You will be provided with the correct answer with detailed explanation after you have completed all the questions.

1. What is security exploitation?

A. An application is prepared to take advantage of a known weakness.
B. How to find information such as username, password and credit card details by forging as a trusted entity in electronic communication.
C. A module is researched by most Computer Science students.
D. Mobile Internet solution

2. What is SQL Injection?

A. A versatile programming language
B. A type of security exploit in which an attacker adds a Structured Query Language (SQL) code to the Web form input box to access resources or make changes to the data.
C. A recorded language based on the prototype, used primarily as a client-side JavaScript, deployed as part of a Web browser to provide enhanced user interfaces and dynamic web pages.
D. An American quiz program in many fields: history, literature, art, popular culture, science, sports, geography, words, and more.

3. How to prevent SQL Injection?

A. 'Sterilize' user input data (make sure that users cannot enter anything other than what they are allowed).
B. Do not use SQL anymore
C. Make your code public.
D. All the above.

4. What is password cracking?

D. A secret word or string of characters is used to authenticate, to prove identity or have access to resources.
E. A term used to describe an intrusion into a network, system, or resource, with or without the use of a tool to unlock a secured resource with a password.
F. An encryption protocol provides secure communication over the Internet.
G. Marking language.

5. What is a "white hat" hacker?

A. One person specializes in penetration testing and other testing methods to ensure the security of an organization's information system.
B. Someone breaks into a computer system or network for bad purposes.
C. A hacker with a white hat.
D. All of the above.

6. What is Packet sniffer?

A. A versatile server-side scripting language designed for the initial purpose of serving web development to create dynamic websites.
B. A set of rules for encoding documents in readable form.
C. An application captures data packets, which can be used to 'catch' passwords and other data when transferred over the network.
D. All of the above.

7. What is cross-site scripting?

A. A programming language that allows controlling one or more applications.
B. A type of computer security vulnerability is often found in Web applications, allowing an attacker to insert client-side scripts into Web pages viewed by other users.
C. A kind of specialized scripting language used to control computers.
D. Documents or information resources are suitable for the World Wide Web and can be accessed via web browser and displayed on the screen or mobile device.

8. What is Social Engineering?

A. The technique causes people to perform certain acts or disclose confidential information.
B. A professional technical discipline involves the design, construction and maintenance of physical and natural environments, including works such as roads, bridges, canals, dams and buildings.
C. A technical discipline applies the principles of physics and materials science to the analysis, design, production and maintenance of mechanical systems.
D. Direct human control of an organism's genome using modern DNA technology.

9. What is Rootkit?

A. A kit used by biologists when working with plants.
B. Default name of UNIX directory.
C. Rootkits are designed to bypass computer security methods.
D. A identifier server for the root area of ??the Domain Name System.It directly responds to requests for records in the root zone and responds to other requests to return a list of authorized identifier servers assigned to the appropriate top-level domain (TLD).

10. What is spoofing attack?

A. A technique in sumo in Japan.
B. A fake attack involves a fake program, system, or website, which successfully performs fake data and is therefore considered a trusted system by the user or another program.The purpose of this is usually to trick

programs, systems or users to disclose confidential information, such as usernames and passwords to attackers.

C. Both

Answers and explanations:

1. A. Security Exploitation (Security Exploitation) is a pre-prepared application to take advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery, which misuse security vulnerabilities that appear due to substandard programming. Other exploits can be used via FTP, HTTP, PHP, SSH, Telnet and some websites. They are very popular in network attacks, websites / domains.

2. B.SQL queries are requirements to perform certain actions on the database.Usually on web forms used to authenticate users, when a user enters a username and password, these values ??will be inserted into the SELECT query.If the entered value is found in the database, the user is allowed access and vice versa, the access request will be denied.If web forms don't have a mechanism to block other input with a username and password, an attacker can use these forms to send their requests to the database.The request may be to download the entire database or interact with it in other unauthorized ways.

3. A. The best way is to carefully censor data entered by users, all data received from users must be considered unsafe.

4. B. Password cracking is the process of recovering passwords from data stored or transmitted in a computer system.The most used method is to constantly try to guess the password.The other way is to report the forgotten password and change it.The purpose of password cracking is to help users recover passwords when forgotten (though setting a new password will bring less security risks, but related to system administration rights), to access Unauthorized access to the system, or used as a preventive measure to help system administrators measure the level of password cracking.

1. Summary of how to create strong passwords and manage the most secure passwords

5. A. The term 'white hat' refers to ethical hackers - ethical hackers, or a computer security expert, specializing in penetration testing and other testing methods to ensure safe for an organization's information system.

6. C. Packet analyzer (also known as network analyzer, protocol analyzer or sniffer, or for specific types of networks, wireless sniffer, Ethernet sniffer) is a Computer programs or a piece of hardware, can block and record traffic across the entire network or part of the network.When the data stream runs through the network, the packet analyzer will 'capture' each packet and if necessary, it will decrypt the raw data of the packet, showing the value of the different fields in the packet for analysis. Its content follows RFC or other appropriate specifications.

7. B. Cross-site scripting (XSS) is a type of computer security vulnerability commonly found in web applications, allowing an attacker to inject code (client side) into a website viewed by other users.XSS vulnerabilities can be used by hackers to bypass access controls such as origin policies.In 2007, Symantec reported 80.5% of XSS-related security attacks.

8. A. Social engineering is a type of attack based on human interaction and often involves manipulating users to circumvent normal security processes, from which an attacker can access the system. , network, physical location or to gain financial benefits.

9. C. Rootkit is designed to bypass antivirus programs on your computer, and can be present in any operating system destructive suite thanks to its legitimate operators.Typically, a rootkit will hide the installer and try to prevent the computer's security system from deleting them.Rootkits can come with replacements of system binaries so that users do not detect an intruder's presence when viewing a list of active processes.

10. B. Spoofing attack is currently very popular on the network.In this type of attack, a person or a software will be forged to falsify data, thereby helping an attacker gain some illegal advantage.3 golden rules to avoid fake attacks

See more:

1. Quiz about security
2. Beginners of computer programming need to focus on what?
3. Testing computer science knowledge, doing little for fun (part 11)