

This chall asks of us to find some answers online. Here they are:

Q1. Which cyber attack tricks users to think that their working stations are infected with malware in order to download malicious software? (Points: 2)

A1. scareware

Q2. In some cases the cyber criminals are gathering information about targets before executing malicious actions. What do we call this type of attack strategy? (Points: 2)

A2. spearphishing

Q3. Which tool is one of the most popular when collecting OSINT intelligence? (Points: 2)

A3. maltego

Q4. From which library can we import functions like printf, scanf, fgets, gets, open, fopen, malloc, free when we want to write a C program? (Points: 2)

A4. libc

Q5. What else can a cheater use to alter game values on a Windows platform? (Points: 2)

A5. cheatengine

Q6. Which is one of the most popular tools used in reverse engineering Android applications? (Points: 2)

A6. apktool

Q7. What type of malware is a program that can continuously replicate itself which causes the infestation of multiple hosts in a very short period of time? (Points: 2)

A7. worm

Q8. What do we call the process which randomizes a set of data in such a way that no algorithm pattern can be deducted? (Points: 2)

A8. entropy

Q9. Which security standard assures that organizations are handling credit card data in a secure manner in order to prevent money fraud and identity theft? (Points: 2)

A9. pcidss

Q10. This type of cyber fraud usually involves use of telephony to execute further phishing attacks. (Points: 2)

A10. vishing

Q11. Which tool is very useful in CTF contests when we need to analyze binaries to discover executable code & embedded files? (Points: 2)

A11. binwalk

Q12. This utility is used to dump TCP traffic on Linux, Windows, Solaris, etc hosts. (Points: 3)

A12. tcpdump

Q13. What is one of the oldest and simplest ciphers that humanity used in the past? (Points: 3)
A13. caesar

Q14. Which function do we use when we want to map arbitrary size data to fixed sized data? (Points: 3)
A14. hashing

Q15. In which country was the Enigma cipher developed? (Points: 3)
A15. germany

Q16. Which framework was developed by security specialists used in penetration tests to assess web applications vulnerabilities? (Points: 3)
A16. w3af

Q17. Which web vulnerability occurs when an application reveals pieces of data to the end-user that shouldn't be public? (Points: 3)
A17. informationleakage

Q18. What do we call the set of rules which monitors and filters the traffic from the Internet and a web application to protect it from different types of cyber attacks like XSS, SQL injection, etc? (Points: 3)
A18. waf

Q19. What is the name of the security incident that occurs when an attacker obtains access to user data? (Points: 3)
A19. databreach

Q20. Which is one of the most popular Python libraries that are used most in CTF contests to develop exploits for the found vulnerabilities? (Points: 3)
A20. Pwntools

Made with love by: AndreiCat