1.What is a blind SQL injection?

A.A helper application for SQL injection developed for the partially sighted

B.A type of attack where the result is not directly visible to attacker

C.When the attacker is only capable of randomly modifying the SQL query

D.When the attacker is only capable of modifying the SQL query with the help of a proxy module

2.Interdependent privacy risks for a given user emerge owing to

A.Negative externalities of data sharing with third parties

B.High fixed costs of ICT services

C.Positive externalities of data sharing with third parties

D.The data sharing decisions of the given user

3.What is Stuxnet?

A.a malware

B.An Iranian uranium enrichment plan

C.An industrial network standard

D.A network of cyber criminal organizations

4.Which of the following solutions can provide protection against ROP attacks?

A.ASLR

B.Harvard architecture

C.DEP

D.NX bit

5.Information security is risk management. Assuming that attackers are becoming more skilled over time and other factors affecting the risk of an attack stay the same,

A.The likelihood of the attack stays the same, but the risk increases

B.The likelihood of the attack increases, hence the risk decreases

C.The likelihood of the attack decreases, hence the risk increases

D.The likelihood of the attack increases, hence the risk increases

6.What does the design principle "complete mediation" say?

A.The amount of shared mechanisms should be minimized

B.Software should run with the least amount of privileges necessary to complete its task

C.Keep it small and simple

D.Check every access to every object every time access is requested

7.Which of the following attacks is not relevant for key exchange protocols?

A.Replay of protocol messages

B.Impersonating a protocol participant

C.Exhaustive key search attack

D.Man-in-the-middle attack

8.Which of the following risks is not relevant for IT security?

A.Denial of services provided by an IT system

B.Illegal access to data

C.Illegal modification of data

D.Random hardware failures

9.What does k-anonymity mean?

A.The direct identifiers of an individual match at least k records in the anonymized dataset

B.The sensitive attribute values of an individual match at least k, or 0 records in the anonymized dataset

C.The quasi-identifiers if an individual match at least k, or 0 records in the anonymized dataset
D.The sensitive attribute values of an individual match at most k records in the anonymized dataset

10.What property of JavaScript makes it dangerous?
A.a user generated event is equivalent to a code-based event
B.Every object inherits from a global prototype
C.The language was developed in about 10 days
D.Every variable is in the global scope

11.What is a shell code?
A.a particular type of message integrity checksums
B.The passcode needed to run the shell
C.The program code of the OS shell (e.g. bash or cmd.exe)
D.Attacker input that aims at opening a shell

12.Which of these is not among the most common attacks against browsers?
A.Stack/heap overflow
B.Use-after-free
C.Integer overflow
D.Compromising the ASLR

13.Which of the following properties characterize cyber criminal groups?
A.Advanced technical skills, variable information gathering capabilities, rich resources
B.Advanced technical skills, advanced information gathering capabilities, limited resources
C.Variable technical skills, limited information gathering capabilities, limited resources
D.Limited technical skills, limited information gathering capabilities, rich resources

14.Which task is to relay security-related info to the development team?
A.Security contact
B.Security advisor
C.Security team
D.Security leadership team

15.What is not among the security goals of Google Chrome?
A.Reducing the spreading of exploits
B.Reducing the frequency of exposures
C.Reducing the window of vulnerabilities
D.Reducing the severity of vulnerabilities

16.What is a stack frame?
A.Pair of memory addresses referring to the top and the bottom of the stack
B.A framework for programming the stack
C.Memory area referenced by the stack pointer
D.Part of the stack handled by a given function when it is called

17.What does the design principle "least common mechanism" say?
A.The amount of shared mechanisms should be minimized
B.Software should run with the least amount of privileges necessary to complete the task
C.Check every access to every object every time access is requested
D.Consider the human in the loop

18.What does salting mean in the case of password hashing?

A.Decreasing the hash computation time by optimization

B.Increasing the hash computation time artificially

C.Computing a hash of random length

D.The hash depends on some random input, besides the password

19.Android device encryption feature protects against which of the following attacks?

A.Reading user data from the memory of a phone that is tuned on

B.Ransomware (since everything is already encrypted)

C.Reading user data from the storage of a phone that is turned on, using a data cable disguised as a
   USB charging cable

D.Reading user data from the flash chip of a phone that is turned off

20.Which of the following statements is FALSE?

A.Developers are faced with constraints during the development process

B.Measuring security is difficult

C.Frameworks used during programming do not help the programmer in his/her work

D.Attackers only need to find a single vulnerability, while developers have to pay attention to
   everything in order for the software to be secure.

21.What is the goal of browser fingerprinting?

A.Identify the browser with cookies

B.Identify the browser with its persistent attributes

C.Identify the user with his/her direct identifiers

D.Identify the browser only with its version number

22.Which of these is not a type of XSS?

A.Reflected XSS

B.Event based XSS

C.DOM based XSS

D.Persistent XSS

23.What is the main cause that computers can be cracked?

A.They contain vulnerabilities

B.No antivirus product is installed

C.Programmers have strict deadlines

D.The appropriate ports are not closed

24.The lemon market for information security is created by

A.Information asymmetry

B.Low demand

C.High fixed costs

D.High marginal costs

25.Which of these is performed as a first step during an IOS boot?

A.The kernel is initialized

B.The Apple root certificate is loaded

C.The iBoot code is checked

D.The low level bootloader is executed

26.Which of the following actions need a dangerous permission on Android?

A.Sending HTTP POST request to the developer's server

B.Turning on the vibrator

C.Turning on the WIFI

D.Sending an SMS

27.What is black-box testing?

A.Checking only the input and the output, fuzzing

B.A pentest where the ethical hacker has the source code

C.A vulnerability testing where we have only minimal information on the target system

D.When we use programs for testing that are not known by the developer

28.Why do we hash messages before signing them?

A.This allows for shorter signature keys

B.This makes the computation of the signature faster

C.This ensures that besides signing, the message is also encrypted

D.This makes it more difficult to forge signatures

29.Which security service is provided by encryption?

A.Confidentiality

B.Non-repudiation

C.Integrity protection

D.Message authentication

30.Zero-day vulnerabilities are...

A.Unpublished vulnerabilities which are known to the attacker

B.Vulnerabilities that can be identified in less than 1 day

C.Vulnerabilities that can be fixed quickly with no effort

D.Publicly well-known Vulnerabilities

31.What is a reference monitor in the model of access control?

A.a dashboard where we can monitor the operation of our access control system

B.An entity that keeps track of the reference to the objects and helps in garbage collection

C.An entity that defines the access control rules

D.An entity that enforces an access control policy

32.What is "lateral movement"?

A.One element of an attack, where attackers go from one infected host to others

B.A jump instruction based on memory load instructions

C.Protected copy of memory arrays

D.Using LM drivers to raise the level of security

33.How does hybrid encryption work?

A.The data is encrypted with an asymmetric key cipher whose key is encrypted with symmetric key cipher

B.The data is encrypted with a symmetric key cipher whose key is encrypted with an asymmetric key cipher

C.We use the DES cipher in an encrypt-decrypt-encrypt mode (i.e. 3DES in EDE mode)

D.We compute a MAC besides encrypting the data (like AES-CCM or AES-GCM)

34.What information can be obtained about a website without loading it or communicating with the server?

A.The kernel's version number

B.The version of the webserver, sometimes even the kind of the operating system
C.The number of running threads
D.The source code of scripts and the security level of the database

35. What is a fingerprint minutiae?
A.Special area of the fingerprint (core or delta)
B.A global fingerprint pattern (such as whirl, loop, arch)
C.The graph defined by the ridge endings and bifurcations
D.(Type (ending or bifurcation), position, direction) triplet

36.Which protocol do we use for accessing web pages securely?
A.WPA2
B.IPsec
C.SSH
D.TLS

37.A database contains the age, home address, and the list of visited locations of individuals. Which of
  these attributes do identify an individual the most in this dataset?
A.Home address and 2 visited locations
B.Age, home address and 2 visited locations
C.Home address
D.Age and 2 visited locations

38.What happens in case of a stack overflow?
A.The computer runs out of stack memory
B.Part of the stack is overwritten in an unexpected way
C.Too much data is pushed on the stack and it overwrites part of the heap memory
D.The return address of a function is overwritten on the stack

---

1.Which of the following programming languages is sensitive for buffer overflow probelms?
A.Python
B.Java
C.Rust
D.C/C++

2.What is a reduction proof in modern cryptography?
A.When we prove that breaking a given cipher is at least as hard as efficiently solving a hard (or
  believed to be hard) mathematical problem
B.When we prove the security of each component of a cipher, from which it follows that the entire
  cipher is ...
C.When we prove that efficiently solving a hard (or believed to be hard) mathematical problem (e.g.
  factoring) ..... breaking a given cipher
D.When we trace back the problem of breaking a given cipher to that of breaking one of its
  components, or .... prove that it is sufficient to break that single component to break the cipher.

3.What is a botnet?
A.a network designed as a fractal for robust calculations
B.Anonymization network with many participants
C.A cluster of computers used for distributed computing (hard math problems)
D.A network of infected computers (also named zombies) made by attackers

4.Most important properties of worm attacks is
A.Needs user interaction and hence spreads slowly
B.Exploiting network Vulnerabilities they replicate rapidly automatically
C.Very hard to detect by antivirus tools as they use polymorphic code
D.Have a very long code structure

5.In fuzzing, the test executor...
A.Does not user error reports
B.Instruments the analyzed piece of software
C.Provides the secure random number generator
D.Collects data about the execution

6.The cascade (vienna) computer virus ...
A.One of the first cyber-physica attacks around 2010
B.Infected DEC machines back in the 1970's
C.Is one of the first brutal worm attacks in the early 2000's
D.Is originating from the 1980's and it made big media coverage

7.What is the purpose of secure Enclave coprocessor?
A.Providing a secure boot for the system
B.Signature checking for applications
C.Recording and storing fitness data
D.Handling the Touch ID sensor

8.What are the links NOT encrypted in TOR?
A.Between the Entry Onion Router and the Onion Proxy
B.Between the Exit Onion Router and the destination
C.Between two Onion Routers
D.Between the Entry and the Exit Onion Routers

9.Which of the following decisions related to software development must concern itself with the
  principle of fail-safe defaults?
A.Deciding how to document the internal structure of the software in the user manual
B.Creation of the user account via which the software can connect to the database
C.Designing the buttons on the GUI
D.Decision concerning the default configuration values