Corrigé DS (tapé à la main par ce cher Patrick Balkany, le roi des roublards)

Hésitez pas à rechecker les questions au cas où :)

1. What is NOT a security service ?

a.Authentification

b. Aviability

c.Confidentiality

d.Integrity

2. An institutional (static) website of a company that wants to promote its services on the internet has security need :

1. Strong in confidentiality
2. Strong in integrity
3. Low in confidentiality
4. Low in integrity

3. What’s doing the User Agent ?

1. telling the version of BIOS system
2. telling a website information about the browser and operating system
3. telling if there is a potential SQL injection
4. telling if you should of souldn’t pass the exam (wtf)

4. What is NOT a security activity ? (réponse par élimination)

1. Détection
2. Mitigation
3. Prévention
4. Protection

5. What is the most important security service ? (me paraît être le plus général des 4, j’hésite avec HTTP (http c’est pas un sécurité service non? cest https). A vérifier !!!

1. DHCP
2. DNS
3. HTTP
4. SNMP (not a service)

6. One is polite, one is not so polite, one is dealing with errors, but which is the remaining one?

1. ICMP
2. IP
3. TPC j’aurai dit ça pcq il dit polite en rapport avec les handshakes du protocol maybe ?
4. UDP

7. An XSS is an injection attack which generally occurs on:

1. Server Side
2. Operator Side
3. Client Side
4. Root Side

8. What does ARP stands for?

1. Address Recovery Protocol
2. Address Recognition Protocol
3. Address Resolution Protocol
4. Address Routing Protocol

9. While troubleshooting a communication issue, it is wise to think:

1. Like a layer
2. Like a lawyer
3. Like a looser
4. Like a lower

10. If I detect the port SQL open and I find a user input to search things like article, which input would I try?

1. ; cat~/etc/passwd
2. <script>alert(“coucou”);</script>
3. ../../../../etc/passwd%00
4. ‘union select username,password from users;

11. If you see in the url target: <http://test.org/> articles/?page=cestfini.php, which attack would you like to test?

1. DDoS Attack
2. XSS (x)
3. SQLi
4. Local File Inclusion (x)

12. What are the fundamental objectives of information security?

1. Data, Information, Criteria, Protocols
2. Duplication, Information, Conformity, Protocols
3. Data, Integrity, Conformity, Evidence (x)
4. Availability, Integrity, Confidentiality, Evidence (x)

13. Risk of the combination of:

1. The severity of an event and its impact
2. The vulnerability and its likelihood
3. The likelihood of an event and its impact (x)
4. The security measures and their impacts

14. A threat is:

1. The potential cause of and incident
2. A weakness in an asset
3. The result of an attack
4. Synonym of vulnerability

15. What does mean “authorization”?

1. Be known by the system
2. Have the right to perform a specific operation
3. Proving who you are
4. Be authenticated by the system

16. In what order are the layers of the OSI model (layer 1-7)?

1. Presentation, Application, Session, Transport, Network, Data Link, Physical
2. Application, Presentation, Session, Transport, Network, Data Link, Physical
3. Physical, Data Link, Network, Transport, Session, Application, Presentation
4. Physical, Data Link, Network, Transport, Session, Presentation, Application

17. The main vector of virus propagation is

1. USB trick
2. Emails
3. Filers
4. Web browsing

18. The network layer of OSI model deals with :

1. Choice of transmission protocol and preparation for sending data specifying the port number used by the application
2. Identification and routing in the network
3. Splitting data into multiple frames
4. Conversion of frames in bits

19. Which transport protocol is connected and have integrity checks?

1. TCP
2. UDP
3. SSL
4. IP

20. A proxy provides:

1. Filtering of applicative streams
2. Filtering of network streams
3. Supervision and logging of web users queries
4. Control of outgoing streams

21. SSH connection:

1. Do not encrypt the communication between the client and the server
2. Sends password in plaintext rendering them susceptible to interception
3. Allows remote login to send instructions on a server
4. Provides confidentiality of data over an unsecured network

22. What equipment do we use to filter TCP/UDP ports and IP addresses?

1. SSL VPN
2. Proxy
3. Firewall
4. Hub

23. A hash:

1. Is used to check a file integrity (can be) true !
2. Allow to encrypt confidential data with a key for later decryption
3. Do not allow to recover the initial data
4. Can be used for storing password

============

24. Asymmetric cryptography *(ou public key cryptography)* :

1. Uses the same key to encrypt and decrypt data
2. Uses a key to encrypt and a different key to decrypt
3. Can quickly encrypt data
4. Is stronger than symmetric cryptography.

25. Symmetric encryption is :

1. An encryption method with two keys
2. An encryption method with one key
3. A fast encryption method
4. A slow encryption method

26. What algorithm allows encrypting data ?

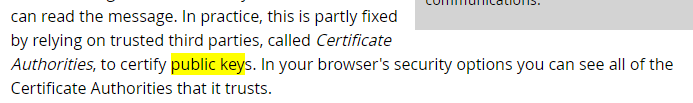
1. Diffie-Hellman
2. AES
3. RSA
4. 3DES

27. What algorithm is used for key distribution ? *(les autres sont des algo d’encryption)*

1. SHA
2. AES
3. Diffie-Hellman
4. RC4

28. Alice wants to communicate with Paul. How can she ensure that she has the correct public key of Paul ?

1. The public key is exchanged by asymmetric cryptography
2. The private key of the sender allows to verify the integrity of the public key used to encrypt the message
3. The public key is encrypted with the message transmitted
4. The digital certificate containing the key is signed by a trusted certification authority



**(Je copie ca ici aussi même s’il ya un autre drive ici :**

[**https://docs.google.com/document/d/1VikpaCwoUpRuwOM5RP7Qy3fh9y9SLrMicdAxX72SBl0/edit**](https://docs.google.com/document/d/1VikpaCwoUpRuwOM5RP7Qy3fh9y9SLrMicdAxX72SBl0/edit)

29) The digital signature:

a. Allows to check data integrity

b. Provides authentication and nonrepudiation of a message

c. Uses the private key to sign, and the public key to verify this signature

d. Uses the public key to sign, and the private key to verify this signature

30) By what process can we have a strong confidentiality?

a. Compression

b. The redundancy of the service

c Encryption

d. Signature

31) A zero-day:

a. Is a vulnerability with no known fix

b. Is a quickly patched security flaw

c. Is a particular malware

d. Is the name of an attack tool

32) What attack can lead to get the cookies from the victim to obtain the credentials or at least the identifier of the session?

a. SQL injection

b. Cross Site Scripting (XSS)

c. DNS Spoofing

d. Man in the Middle

33) The deepweb:

a. Represent 4% of all information on the Web

b. Is a set of pages not referenced by search engines // je pense que c’est juste

c. Can only be accessed with specific tool (You don't need any special tools or a dark net browser to access the deep web; you just need to know where to look)

d. Use specific extensions (.onion) (non ca c’est le dark web)

34) The Onion Router :

a. Use relays that only know the IP address of two other relays ( noeud précdent et noeud suivant)

b. Is a network of proxy servers

c.- used to hide the clients IP address to the targeted website

Concrètement, **TOR est un réseau multi-proxy** qui ne repose pas sur des serveurs proxy spécifiques pour traiter les données. A la place, il **utilise les connexions d’une multitude d’autres utilisateurs** de TOR afin de masquer l’IP de l’utilisateur original. Sachant que plus de 3 millions d’utilisateurs partagent leurs IP dans le monde entier, le risque de retrouver la provenance d’origine d’une requête internet est pratiquement impossible.

d. Offers as much anonymity as a VPN (Le navigateur Tor permet aussi à ses utilisateurs de pénétrer dans ce qu'on appelle parfois le Dark Web , dans une discrétion absolue et sans le besoin d'utiliser un VPN ou un Proxy)

35) Thè Onion Router browser:

a. Need to use HTTPS in order to avoid MITM

b. Can use javascript

c. Can be detected and forbidclen on some websites

d. Is used to access hidden services

36 Hidden service:

a. Sends a service descriptor to the introduction point

b. Signs the descriptor with the service's private key

c. Is accessible by requesting a 16-character narre derived from the public key of the service d Sends its public key to the rendezvous point

37) The customer of a hidden service:

a. Uses the private key of the service to encrypt the address of the rendezvous point

b. Sends a one-time secret to the introduction point

c. Communicates with TOR service

d. Checks if the service exists in distributed hash table

38) The blockchain :

a. 1s only used for digital currency

b. is a technology of storage and transmission without control system

c. Needs human intervention to be regulate

d. Is a public registry for all transactions made since the start of the distributed system

39) Bitcoin:

a. Will be limited to 21 million units

b. Uses a general organization which is totally public

c. ls a safe investment for long-term savings

d. Uses cryptographic algorithms to pay and receive payments

40) Miner:

a. Has to salve a brute force cryptography problem to add blocks to the chain

b. is paid for hvs work when he finds a hash of the previous block

c. ls paid with the generation of a certain amount of cryptocurrency and/or transaction fee

d. Is an entity whose role is to update the decentralized database

allintitle: Confidential filetype:pdf

[confidential site:ece.fr] filtetype:pdf

Intitle plutot que allintitle, je pense