Cyber Security Quiz 1

Name:
Student Code:

MCQ (choose ALL the correct answers)

1) In Past times (70s) "hacking" was done …. :
    a) Physically
    b) Programmatically
    c) Using social engineering
    d) Using Metasploit framework

Answer: a, c

2) The Egyptian police promised an American spy a large villa and an annual check of $100k if he told the government about the new alien spaceship research.
   The American spy told them that aliens are real and handed them classified documents and took the paycheck.
   However the "aliens" he was referring to were just some bacteria living on Mars.

   The government and the smart spy both used …..:
    a) Elicitation
    b) Mind Tricks
    c) Pretexting
    d) Violence

Answer: b

3) We study how to use destructive tools in the cyber security course:
    a) Because a good defender must know his enemy
    b) To be able to change/secure the top assets at the pyramid of pain
    c) To destruct organizations and make them lose money
    d) To enter a local group of cool hackers

Answer: a, b

4) Automated vulnerability assessment and manual pentesting:
    a) Are used both
    b) Having only one of them is enough
    c) Having using both is not enough and we still need more expertise
    d) Only one of them should be used, because both yield the same results.

Answer: a

5) Top secret documents have been leaked, the CIA triad side that has been violated is:
    a) Confidentiality
    b) Integrity
    c) Availability

Answer: a

6) From the disadvantages of Bell La-Padula model is
    a) Slowness
    b) Low confidentiality, as anyone can write up
    c) That it assumes all data is already classified, everyone knows his own responsibilities
    d) No flexibility, roles will not change in the organization.

Answer: a, c, d

7) PIM and PAM are used to preserve ….:
    a) Confidentiality
    b) Availability
    c) Human efforts
    d) None

Answer: a

8) The login page of a website authorizes user credentials by looking up a database of registered users, and in front of each user there is his role in the system, should it

be admin or supervisor or sys owner, etc.
This process uses ….:

a) PIM
b) PAM
c) Pyramid of Pain
d) DDoS

Answer: b

9) Biba model achieves:
   a) Confidentiality
   b) Integrity
   c) Sanity
   d) Flexibility

Answer: b, d

10) A new malware is just disclosed!
    In order to come up with a suitable anti-virus and further secure our devices, the malware analyst will do:
    a) Preparation → Identification ← → Mitigation → Review
    b) Review → Mitigation → Identification → post-attack review
    c) Mitigation → Review → Mitigation → Review and so on
    d) Download virus_eradicator_3000_warhead.exe

Answer: a

11) Assets at the top of the pyramid of pain are “hard” because:
    a) It is hard for us CS engineers to mitigate the attack but very easy for the attacker to attack using a different asset
    b) It is easy for us CS engineers to mitigate the attack, but very hard for the attacker to change his used assets, that’s why it is the pyramid of pain for hackers.
    c) It is hard for CS engineers to mitigate the attack, but if we successfully mitigated this asset, it would be very hard for the attacker to change the used asset.
    d) The assets at the top are numerous, that’s why they are called hard.

Answer: c

12) You notice unusual traffic coming from a certain IP address, so you just block this IP address.
However after doing this, the same unusual traffic came from another different IP address, so you also block the new one.
You, and the attacker are doing something wrong which is:
    a) Focusing on changing an asset at the bottom of the pyramid of pain
    b) Using a hard task, grinding
    c) Not setting up a proper Intrusion Detection System -IDS- and the attacker is using a cheap automatic VPN

Answer: a, c

13) If you find an open port, 80, with HTTP service running on it, suppose the machine's IP is 250.60.100.2
this indicates you can extract some info by:
    a) Sending remote code to be executed on the target machine
    b) Possibly opening a website by typing "250.60.100.2 : 80" at the URL bar in your browser
    c) Getting the number of users and possibly know the root/sudo user of the target machine

Answer: b

14) Initially, each node in the network knows a little bit of topology of the network:
    a) True
    b) False

Answer: b

15) A node registers its neighbors using a ….. Packet:
    a) SYN
    b) Routing table
    c) HELLO
    d) ACK

Answer: c

16) The packet that is passed to the neighbors during the link state protocol is the ……:
    a) Routing table
    b) Machine Metadata (system owner, system registrar, etc.)
    c) Domain name
    d) SYN/ACK

Answer: a

17) Choosing TCP or UDP is managed by:
    a) Network layer
    b) Data Link and Physical
    c) Application layer
    d) Transport

Answer: d

18) Ensuring the data packet is correctly delivered from source to destination, aka routing is done by:
    a) Application layer
    b) Network layer
    c) Data Link and physical layer
    d) Application layer

Answer: b

19) A TCP block of data inside the transport layer is not referred to as just “data”, the correct terminology is:
    a) Datagram
    b) Packet
    c) Frame
    d) Segment

Answer: d

20) Using NAT, if a packet is coming from the outside Internet, and wants to enter a certain computer inside the LAN, the ….. Is used to correctly direct the packet:
    a) Target machine's MAC address, (the target machine is the dst machine inside the LAN)
    b) Port number of the source machine (the sender machine)
    c) TTL field inside the packet
    d) Port number at which the target machine is connected to the LAN's router

Answer: d

21) What if a router received a packet and its TTL = zero?
    a) The router discards the packet
    b) The router floods the packet Two times only
    c) The router floods the packet but first, increments the TTL then sends it
    d) Send the packet back to where it came from, the packet contains reverse path

Answer: a

22) IPv6 is:
    a) 32 bits
    b) 64 bits
    c) 128 bits
    d) 256 bits

Answer: c

23) IANA gave you this: 245.0.0.0 with another number: 255.0.0.0,
The first number is:
    a) Subnet mask
    b) IPv4 address
    c) Subnet
    d) Number of IPs

Answer: c

24) From the previous question, you conclude how many unique IPs are usable?
    a) 256
    b) 32 * 32
    c) 256 * 256 * 256
    d) 256 * 256 * 256 * 256

Answer: c

25) Visiting a Webpage, sending a GET request then receiving a response, is a form of:
    a) Active recon
    b) Passive recon
    c) Elicitation

Answer: a

26) Anti Virus systems can catch nmap:
    a) True
    b) False

Answer: b

27) Transport Layer treats the network as a black box, it doesn't care about mini details as hops, correctness, etc:
    a) True
    b) False

Answer: a

28) NMAP can be caught for anomalous traffic easily when we use the -A argument?
    a) True
    b) False

Answer: a

29) Why do we use nmap?
    a) Because some creep forces us to
    b) Because it is helpful during the pentesting cycle

c) To force open a port to send remote commands
d) To know the topology and assess the target for entry points

Answer: b, d

30) Normally when no IDS is up, you can just use … flag to gain the maximum knowledge and perform all scans about the target regardless of the sent traffic or the taken time.
a) -A
b) -vv
c) -sS
d) -PA

Answer: a

31) gcd(24, 30, 36)
a) 2
b) 3
c) 5
d) 6

Answer: d

32) Find the multiplicative inverse of 3 mod 5
a) 3
b) 5
c) 2
d) 15

Anser: c

33) Encrypt this message using Caesar Cypher, m=”IAMBATMAN” with key = -1
a) HZLAZSLZM
b) JBNCBUNBO
c) CBUNBOJBN
d) AZSLZMHZL

Answer: a

34) DES is simpler than AES (but not necessarily faster). Why not use triple DES instead of a single AES?
    a) Triple DES is not as secure as AES
    b) Triple DES is very slow
    c) We will use double DES to get best of both worlds
    d) Because NIST said AES is the new international standard in TLS handshake and is the new used cryptographic standard.

Answer: a, b, d

35) From the requirements of the Hash function:
    a) Very little collisions, or near zero
    b) Fixed output length for variable input length
    c) Must be complex, so no analyst can find a reverse way (to make the hash function 1-way only)
    d) To be as fast as possible

Answer: a, b, c, d

State 1 difference between:

1) Nslookup and nmap

2) Hash and encryption

3) OSI and TCP/IP

Scenario Question

A cyber attack happened at the faculty!!
Eng. Goku calls the …… team as soon as the attack happens
Then shortly after the attack is finished, the …… team arrived
After 4 days of police investigations, the attacker was finally caught.

Then prof. Jotaro swore this will not happen again, and hired a reliable ……. Team to further secure the website and aid developers.

[Pentesting, Malware analyst, Incident response, body guard, info sec, forensics]

Answer: Incident Response, Forensics, Pentesting