Question Bank for Information and Cyber Security (ICS)

1. Why would a hacker use a proxy server?
A. To create a stronger connection with the target.
B. To create a ghost server on the network.
C. To obtain a remote access connection.
D. To hide malicious activity on the network.

Correct Answer – D
Explanation – Proxy servers exist to act as an intermediary between the hacker and the target and servces to keep the hacker anonymous tot he network.
2. What type of symmetric key algorithm using a streaming cipher to encrypt information?
A. RC4
B. Blowfish
C. SHA
D. MD5

Correct Answer – A
Explanation – RC$ uses streaming ciphers.
3. Which of the following is not a factor in securing the environment against an attack on security?
A. The education of the attacker
B. The system configuration
C. The network architecture
D. The business strategy of the company
E. The level of access provided to employees

Correct Answer – D
Explanation – All of the answers are factors supporting the exploitation or prevention of an attack. The business strategy may provide the motivation for a potential attack, but by itself will not influence the outcome.
4. What type of attack uses a fraudulent server with a relay address?
A. NTLM
B. MITM
C. NetBIOS
D. SMB

Correct Answer – B
Explanation – MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.
5. What port is used to connect to the Active Directory in Windows 2000?
A. 80
B. 445
C. 139
D. 389

Correct Answer – D
Explanation – The Active Directory Administration Tool used for a Windows 2000 LDAP client uses port 389 to connect to the Active Directory service.
6. To hide information inside a picture, what technology is used?
A. Rootkits
B. Bitmapping

C. Steganography
D. Image Rendering

Correct Answer – C
Explanation – Steganography is the right answer and can be used to hide information in pictures, music, or videos.
7. Which phase of hacking performs actual attack on a network or system?
A. Reconnaissance
B. Maintaining Access
C. Scanning
D. Gaining Access

Correct Answer – D
Explanation – In the process of hacking, actual attacks are performed when gaining access, or ownership, of the network or system. Reconnaissance and Scanning are information gathering steps to identify the best possible action for staging the attack. Maintaining access attempts to prolong the attack.
8. Attempting to gain access to a network using an employee's credentials is called the _____________ mode of ethical hacking.
A. Local networking
B. Social engineering
C. Physical entry
D. Remote networking

Correct Answer – A
Explanation – Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.
9. Which Federal Code applies the consequences of hacking activities that disrupt subway transit systems?
A. Electronic Communications Interception of Oral Communications
B. 18 U.S.C. § 1029
C. Cyber Security Enhancement Act 2002
D. 18 U.S.C. § 1030

Correct Answer – C
Explanation – The Cyber Security Enhancement Act 2002 deals with life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems.
10. Which of the following is not a typical characteristic of an ethical hacker?
A. Excellent knowledge of Windows.
B. Understands the process of exploiting network vulnerabilities.
C. Patience, persistence and perseverance.
D. Has the highest level of security for the organization.

Correct Answer – D
Explanation – Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.
11. What is the proper command to perform an Nmap XMAS scan every 15seconds?
A. nmap -sX -sneaky
B. nmap -sX -paranoid
C. nmap -sX -aggressive
D. nmap -sX -polite

Correct Answer – A
Explanation – SX is used to identify a xmas scan, while sneaky performs scans 15 seconds apart.

12. What type of rootkit will patch, hook, or replace the version of system call in order to hide information?
A. Library level rootkits
B. Kernel level rootkits
C. System level rootkits
D. Application level rootkits

Correct Answer – A
Explanation – Library leve rootkits is the correct answer. Kerel level focuses on replaceing specific code while application level will concentrate on modifying the behavior of the application or replacing application binaries. The type, system level, does not exist for rootkits.
13. What is the purpose of a Denial of Service attack?
A. Exploit a weakness in the TCP/IP stack
B. To execute a Trojan on a system
C. To overload a system so it is no longer operational
D. To shutdown services by turning them off

Correct Answer – C
Explanation – DoS attacks force systems to stop responding by overloading the processing of the system.
14. What are some of the most common vulnerabilities that exist in a network or system?
A. Changing manufacturer, or recommended, settings of a newly installed application.
B. Additional unused features on commercial software packages.
C. Utilizing open source application code
D. Balancing security concerns with functionality and ease of use of a system.

Correct Answer – B
Explanation – Linux is an open source code and considered to have greater security than the commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist. Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack.
15. What is the sequence of a TCP connection?
A. SYN-ACK-FIN
B. SYN-SYN ACK-ACK
C. SYN-ACK
D. SYN-SYN-ACK

Correct Answer – B
Explanation – A three-handed connection of TCP will start with a SYN packet followed by a SYN-ACK packet. A final ACK packet will complete the connection.
16. What tool can be used to perform SNMP enumeration?
A. DNSlookup
B. Whois
C. Nslookup
D. IP Network Browser

Correct Answer – D
Explanation – SNMPUtil and IP Network Browser is SNMP enumeration tool
17. Which ports should be blocked to prevent null session enumeration?
A. Ports 120 and 445
B. Ports 135 and 136
C. Ports 110 and 137
D. Ports 135 and 139

Correct Answer – D
Explanation – Port 139 is the NetBIOS Session port typically can provide large amounts of information using APIs to connect to the system. Other ports that can be blocked in 135, 137,138, and 445.
18. The first phase of hacking an IT system is compromise of which foundation of security?
A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Correct Answer – B
Explanation – Reconnaissance is about gathering confidential information, such as usernames and passwords.
19. How is IP address spoofing detected?
A. Installing and configuring a IDS that can read the IP header
B. Comparing the TTL values of the actual and spoofed addresses
C. Implementing a firewall to the network
D. Identify all TCP sessions that are initiated but does not complete successfully

Correct Answer – B
Explanation – IP address spoofing is detectable by comparing TTL values of the actual and spoofed IP addresses
20. Why would a ping sweep be used?
A. To identify live systems
B. To locate live systems
C. To identify open ports
D. To locate firewalls

Correct Answer – A
Explanation – A ping sweep is intended to identify live systems. Once an active system is found on the network, other information may be distinguished, including location. Open ports and firewalls.
21. What are the port states determined by Nmap?
A. Active, inactive, standby
B. Open, half-open, closed
C. Open, filtered, unfiltered
D. Active, closed, unused

Correct Answer – C
Explanation – Nmap determines that ports are open, filtered, or unfiltered.
22. What port does Telnet use?
A. 22
B. 80
C. 20
D. 23

Correct Answer – D
Explanation – Telnet uses port 23.
23. Which of the following will allow footprinting to be conducted without detection?
A. PingSweep
B. Traceroute
C. War Dialers
D. ARIN

Correct Answer – D
Explanation – ARIN is a publicly accessible database, which has information that could be valuable. Because it is public, any attempt to obtain information in the database would go undetected.
24. Performing hacking activities with the intent on gaining visibility for an unfair situation is called ________.
A. Cracking
B. Analysis
C. Hacktivism
D. Exploitation

Correct Answer – C
Explanation – Hacktivism is the act of malicious hacking for a cause or purpose.
25. What is the most important activity in system hacking?
A. Information gathering
B. Cracking passwords
C. Escalating privileges
D. Covering tracks

Correct Answer – B
Explanation – Passwords are a key component to access a system, making cracking the password the most important part of system hacking.
26. A packet with no flags set is which type of scan?
A. TCP
B. XMAS
C. IDLE
D. NULL

Correct Answer – D
Explanation – A NULL scan has no flags set.
27. Sniffing is used to perform ______________ fingerprinting.
A. Passive stack
B. Active stack
C. Passive banner grabbing
D. Scanned

Correct Answer – A
Explanation – Passive stack fingerprinting uses sniffing technologies instead of scanning.
28. Phishing is a form of ____________________.
A. Spamming
B. Identify Theft
C. Impersonation
D. Scanning

Correct Answer – C
Explanation – Phishing is typically a potential attacker posing, or impersonating, a financial institution
29. Why would HTTP Tunneling be used?
A. To identify proxy servers
B. Web activity is not scanned
C. To bypass a firewall
D. HTTP is a easy protocol to work with

Correct Answer – C
Explanation – HTTP Tunneling is used to bypass the IDS and firewalls present on a network.

30. Which Nmap scan is does not completely open a TCP connection?
A. SYN stealth scan
B. TCP connect
C. XMAS tree scan
D. ACK scan

Correct Answer – A
Explanation – Also known as a "half-open scanning," SYN stealth scan will not complete a full TCP connection.
31. What protocol is the Active Directory database based on?
A. LDAP
B. TCP
C. SQL
D. HTTP

Correct Answer – A
Explanation – Active4 direction in Windows 200 is based on a Lightweight Directory Access Protocol (LDAP).
32. Services running on a system are determined by _____________.
A. The system's IP address.
B. The Active Directory
C. The system's network name
D. The port assigned

Correct Answer – D
Explanation – Hackers can identify services running on a system by the open ports that are found.
33. What are the types of scanning?
A. Port, network, and services
B. Network, vulnerability, and port
C. Passive, active, and interactive
D. Server, client, and network

Correct Answer – B
Explanation – The three types of accepted scans are port, network, and vulnerability.
34. Enumeration is part of what phase of ethical hacking?
A. Reconnaissance
B. Maintaining Access
C. Gaining Access
D. Scanning

Correct Answer – C
Explanation – Enumeration is a process of gaining access to the network by obtaining information on a user or system to be used during an attack.
35. Keyloggers are a form of ______________.
A. Spyware
B. Shoulder surfing
C. Trojan
D. Social engineering

Correct Answer – A
Explanation – Keyloggers are a form of hardware or software spyware installed between the keyboard and operating system.
36. What are hybrid attacks?

A. An attempt to crack passwords using words that can be found in dictionary.
B. An attempt to crack passwords by replacing characters of a dictionary word with numbers and symbols.
C. An attempt to crack passwords using a combination of characters, numbers, and symbols.
D. An attempt to crack passwords by replacing characters with numbers and symbols.

Correct Answer – B
Explanation – Hybrid attacks do crack passwords that are created with replaced characters of dictionary type words.
37. Which form of encryption does WPA use?
A. Shared key
B. LEAP
C. TKIP
D. AES

Correct Answer – C
Explanation – TKIP is used by WPA
38. What is the best statement for taking advantage of a weakness in the security of an IT system?
A. Threat
B. Attack
C. Exploit
D. Vulnerability

Correct Answer – C
Explanation – A weakness in security is exploited. An attack does the exploitation. A weakness is vulnerability. A threat is a potential vulnerability.
39. Which database is queried by Whois?
A. ICANN
B. ARIN
C. APNIC
D. DNS

Correct Answer – A
Explanation – Who utilizes the Internet Corporation for Assigned Names and Numbers.
40. Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?
A. Web-based
B. Human-based
C. User-based
D. Computer-based

Correct Answer – D
Explanation – Whether using email, a fake website, or popup to entice the used, obtaining information from an individual over the Internet is a computer-based type of social engineering

1) You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,

```
A  =  [  4  2
         2  1 ]
```

Is the given matrix 'A', a valid key to be used for encryption?

a. Yes
b. No
c. Can't be determined
d. Data insufficient

Answer: b) No

Explanation:

For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist. Here, in this case,

```
| A | = 0
```

Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the Hill cipher.

2) The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

a. The input text is divided into two parts: one being left half and another one being right half.
b. Swapping of the left and right halves are performed after each round.
c. The plain text is converted into a matrix form first
d. None of the above

Answer: c) The plain text is converted into a matrix form first

Explanation:

The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

3) Among the following given options, chose the strongest encryption technique?

a. DES (Data Encryption Standard)
b. Double DES
c. Triple DES
d. AES (Advance Encryption Standard)

Answer: d) AES (Advance Encryption Standard)

Explanation:

It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

4) What is the full-form of RSA in the RSA encryption technique?

a. Round Security Algorithm
b. Rivest, Shamir, Adleman
c. Robert, Shamir, Addie
d. None of the above

Answer: b) Rivest, Shamir, Adleman

Explanation:

The RSA algorithm was named after the three scientists who developed this technique and the name RSA is itself the abbreviation of their names: Rivest, Shamir, and Adleman.

5) Consider the following steps,

i. Substitution bytes
ii. Shift Rows
iii. Mix columns
iv. Add round key

The above steps are performed in each round of which of the following ciphers?

a. Rail fence cipher
b. Data Encryption Standard (DES)
c. Advance Encryption Standard (AES)
d. None of the above

Answer: c) Advance Encryption Standard (AES)

Explanation:

Each round of AES includes the mentioned steps.

1) What is the block size of plain text in SHA- 512 algorithm?

a. 512 bits
b. 1024 bits
c. 2048 bits

d. None of the above

Answer: b. 1024 bits

Explanation:

The SHA- 512 algorithm uses blocks of plain text one at a time to encrypt them into ciphertext. The size of each block in the SHA- 512 algorithm is 1024 bits.

2) All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?

i. Substitution bytes
ii. Shift rows
iii. Mix columns
iv. Add round key

Options

a. i.
b. iii.
c. All of the mentioned
d. None of the mentioned

Answer: b. iii.

Explanation:

In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.

3) What does IDEA stand for in the world of cryptography?
or
The IDEA word in the IDEA algorithm is the abbreviation for which of the following?

a. Independent Decryption Environment Analysis
b. International Defense Encryption Area
c. International Data Encryption Algorithm
d. None of the above

Answer: c. International Data Encryption Algorithm

Explanation:

The IDEA Algorithm stands for "International Data Encryption Algorithm".

4) How many sub-keys in the total are used by the IDEA for encrypting the plain text into ciphertext?

a. 64 sub- keys
b. 48 sub- keys
c. 52 sub- keys
d. Only one key and no subkeys

Answer: c. 52 sub- keys

Explanation:

There are a total of 8 rounds in the IDEA technique for encryption and each of them uses 6 keys. Apart from that, 4 extra keys are used in the final round that is the output transformation round. This gives us a total of 52 subkeys.
(8 x 6) + 4 = 52

5) "The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?

a. 128 key size: 10 rounds
b. 192 key size: 12 rounds
c. 256 key size: 14 rounds
d. All of the above

Answer: d. All of the above

Explanation:

All the mentioned options display the correct relation between the number of rounds and the key size used in the AES algorithm.

6) Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?

a. Avalanche effect
b. Completeness
c. Both a. and b.
d. None of the above

Answer: c. Both a. and b.

Explanation:

Avalanche effect and Completeness are the two characteristic properties of Block ciphers which differ them from stream ciphers.

81.	Public key encryption/decryption is not preferred because
a.	it is slow

b. it is hardware/software intensive

c. it has a high computational load

d. all of the mentioned

View Answer Report Discuss Too Difficult! Search Google

Answer: (d).all of the mentioned

82. Which one of the following is not a public key distribution means?

a. Public-Key Certificates

b. Hashing Certificates

c. Publicly available directories

d. Public-Key authority

View Answer Report Discuss Too Difficult! Search Google

Answer: (b).Hashing Certificates

83. What is the PGP stand for?

a. Permuted Gap Permission

b. Permuted Great Privacy

c. Pretty Good Permission

d. None of the mentioned

View Answer Report Discuss Too Difficult! Search Google

Answer: (d).None of the mentioned

84. PGP makes use of which cryptographic algorithm?

a. DES

b. AES

c.	RSA
d.	Rabin

View Answer Report Discuss Too Difficult! Search Google

Answer: (c).RSA

85.	USENET is related to which of the following Public Key distribution schemes?
a.	Public-Key Certificates
b.	Public announcements
c.	Publicly available directories
d.	Public-Key authority

View Answer Report Discuss Too Difficult! Search Google

Answer: (b).Public announcements

86.	Which of the following public key distribution systems is most secure?
a.	Public-Key Certificates
b.	Public announcements
c.	Publicly available directories
d.	Public-Key authority

View Answer Report Discuss Too Difficult! Search Google

Answer: (a).Public-Key Certificates

87.	Which systems use a timestamp? i) Public-Key Certificates ii) Public announcements iii) Publicly available directories iv) Public-Key authority
a.	i) and ii)

b.	iii) and iv)
c.	i) and iv)
d.	iv) only

View Answer Report Discuss Too Difficult! Search Google

Answer: (c).i) and iv)

88.	Which of these systems use timestamps as an expiration date?
a.	Public-Key Certificates
b.	Public announcements
c.	Publicly available directories
d.	Public-Key authority

View Answer Report Discuss Too Difficult! Search Google

Answer: (a).Public-Key Certificates

89.	Which system uses a trusted third party interface?
a.	Public-Key Certificates
b.	Public announcements
c.	Publicly available directories
d.	Public-Key authority

View Answer Report Discuss Too Difficult! Search Google

Answer: (a).Public-Key Certificates

90.	Publicly Available directory is more secure than which other system?
a.	Public-Key Certificates
b.	Public announcements

c. Public-Key authority

d. None of the mentioned

View Answer Report Discuss Too Difficult! Search Google

Answer: (b).Public announcements

1. A method used by an IDS that involves checking for a pattern to identify unauthorized activity*(No Answer)*

   a. **CORRECT:** Pattern Matching

   b. Session Splicing

   c. Protocol Decoding

   d. State Table

2. A list or table of stored by a router (or switch) that controls access to and from a network.*(No Answer)*

   . State Table

   a. **CORRECT:** Access Control List (ACL)

   b. Session Splicing

   c. Packet Filter

3. An analysis method used by some IDS that looks for instances that are not considered normal behavior.*(No Answer)*

   . Stateful Inspection

   a. **CORRECT:** Anomaly Detection

   b. Evasion

   c. Pattern Matching

4. Bypassing a device, or performing another action, to attack or place malware on a target network without being detected.*(No Answer)*

   . Packet Filter

   a. State Table

   b. **CORRECT:** Evasion

   c. Honeypot

5. A type of firewall closely related to a packet filter that can track the status of a connection through use of a state table that keeps track of connection activities.*(No Answer)*

. Anomaly Detection

a. Protocol Decoding

b. **CORRECT:** Stateful Inspection

c. State Table

6. A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator.*(No Answer)*

. Anomaly Detection

a. Access Control List (ACL)

b. **CORRECT:** Intrusion Detection System (IDS)

c. Session Splicing

7. A type of stateless inspection used in some routers and firewalls to limit flow of traffic to what is on the ACL.*(No Answer)*

. **CORRECT:** Packet Filter

a. Proxy Server

b. Evasion

c. State Table

8. A way of looking at raw packet data.*(No Answer)*

. Proxy Server

a. Session Splicing

b. **CORRECT:** Protocol Decoding

c. Pattern Matching

9. A server (or application) that intercepts the requests clients make of another server, fills the requests that it can, and then forwards the requests it can't handle on to the other server thus helping to improve performance and security.*(No Answer)*

. Honeypot

a. **CORRECT:** Proxy Server

b. Packet Filter

c. State Table

10. A table in which data about connection activity is kept by a stateful firewall.*(No Answer)*

. Evasion

a. **CORRECT:** State Table

b. Honeypot

c. Proxy Server

11. Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network; it logs keystrokes, provides other information about an attacker, and also provides warning that someone is trying to attack your network.*(No Answer)*

. Proxy Server

a. State Table

b. Evasion

c. **CORRECT:** Honeypot

12. A way to change network address information in IP packet headers with a router by connecting multiple computers using one IP address connected to the Internet (or IP network) to convert many private addresses into one public address.*(No Answer)*

. Access Control List (ACL)

a. **CORRECT:** Network Address Translation (NAT)

b. Anomaly Detection

c. Intrusion Detection System (IDS)

13. A method of avoiding detection by an IDS by sending portions of a request in different packets.*(No Answer)*

. **CORRECT:** Session Splicing

a. Protocol Decoding

b. Pattern Matching

c. Evasion

1.
What are drawbacks of the host based IDS ?

□ **A.)** Unselective logging of messages may increase the audit burdens

□ **B.)** Selective logging runs the risk of missed attacks

□ **C.)** They are very fast to detect

□ **D.)** They have to be programmed for new patterns

Show Answer
Answer: Option 'A'
Unselective logging of messages may increase the audit burdens

2.
What are the different ways to classify an IDS ?

□ **A.)** Zone based

□ **B.)** Host & Network based

□ **C.)** Network & Zone based

□ **D.)** Level based

Show Answer
Answer: Option 'B'
Host & Network based

3.
What is major drawback of anomaly detection IDS ?

□ **A.)** These are very slow at detection

□ **B.)** It generates many false alarms

□ **C.)** It doesn’t detect novel attacks

□ **D.)** None of the mentioned

Show Answer
Answer: Option 'B'
It generates many false alarms

4.
What are strengths of the host based IDS?

□ **A.)** Attack verification

□ **B.)** System specific activity

□ **C.)** No additional hardware required

□ **D.)** All of the mentioned

Show Answer
Answer: Option 'D'
All of the mentioned

5.
What are major components of intrusion detection system?

□ **A.)** Analysis Engine

□ **B.)** Event provider

□ **C.)** Alert Database

□ **D.)** All of the mentioned

Show Answer
Answer: Option 'D'
All of the mentioned

6.
What are strengths of the host based IDS?

□ **A.)** Attack verification

□ **B.)** System specific activity

□ **C.)** No additional hardware required

□ **D.)** All of the mentioned

Show Answer
Answer: Option 'D'
All of the mentioned

7.
What are characteristics of stack based IDS ?

□ **A.)** They are integrated closely with the TCP/IP stack and watch packets

□ **B.)** The host operating system logs in the audit information

□ **C.)** It is programmed to interpret a certain series of packets

□ **D.)** It models the normal usage of network as a noise characterization

Show Answer
Answer: Option 'A'
They are integrated closely with the TCP/IP stack and watch packets

8.
What are major components of intrusion detection system?

□ **A.)** Analysis Engine

□ **B.)** Event provider

□ **C.)** Alert Database

□ **D.)** All of the mentioned

Show Answer
Answer: Option 'D'
All of the mentioned

9.
What are characteristics of Network based IDS ?

□ **A.)** They look for attack signatures in network traffic

□ **B.)** Filter decides which traffic will not be discarded or passed

□ **C.)** It is programmed to interpret a certain series of packet

□ **D.)** It models the normal usage of network as a noise characterization

Show Answer
Answer: Option 'A'
They look for attack signatures in network traffic

10.
What are the different ways to classify an IDS ?

□ **A.)** Zone based

□ **B.)** Host & Network based

□ **C.)** Network & Zone based

□ **D.)** Level based

Show Answer
Answer: Option 'B'
Host & Network based

11.
What is major drawback of anomaly detection IDS ?

□ **A.)** These are very slow at detection

□ **B.)** It generates many false alarms

□ **C.)** It doesn’t detect novel attacks

□ **D.)** None of the mentioned

Show Answer
Answer: Option 'B'
It generates many false alarms

1. -systematic tracking of incoming and outgoing traffic: to ascertain how an attack was carried out or how an event occurred on a network.

   -intruders and network users often leave trail behind

   -identify locations where relevant digital evidence exists

   -crucial when developing data map of digital evidence*(No Answer)*

a. SIM Cards

b. Windows Registry

c. **CORRECT:** Network Forensics

d. Drive Slack

2. -personal digital assistant: can be separated devices from mobile phones

   -PDA houses a microprocessor, ROM, RAM, disk drive and various components

   -most common PDA, although not referred to as such:IPAD*(No Answer)*

. Partition

a. SIM Cards

b. EEPROM

c. **CORRECT:** PDA's

3. -a logical drive*(No Answer)*

. EEPROM

a. PDA's

b. SIM Cards

c. **CORRECT:** Partition

4. - .EVE -> .DFT -> IOLogErrors

   -.DD -> .DFT -> IOLogErrors -> MD5*(No Answer)*

. Additional SIM Card Perposes

a. Types of The Formats ProDiscover Creates

b. **CORRECT:** Files Found When Acquisition is Done (ProDiscover)

c. Mobile Forensics Equiptment

5. -allows you to create a representation of another computer on an existing physical computer.

   -a virtual machine is just a few files on your hard drive: must allocate space to it; dynamic or static

   -a virtual machine recognizes components of the physical machine its on: virtual OS is limited by the physical machines O/S and RAM.*(No Answer)*

. Partition

   a. **CORRECT:** Virtual Machine

   b. Drive Slack

   c. SIM Cards

6. Considerations
   -determine the scope of the investigation.
   -determine what the case requires
   -whether you should collect all info
   -what to do in case of scope creep

   the key is to start with a plan but remain flexible in the face of new evidence(No Answer)*

. **CORRECT:** Examination Plan

   a. Drive Slack

   b. Partition

   c. SIM Cards

7. Can be exported as:
   -RTF ~good for thumbnails and book marks
   -TEXT~plain text*(No Answer)*

. Drive Slack

   a. Write Blockers

   b. Windows Registry

   c. **CORRECT:** ProDiscover Report

8. -UNIX DD~most common raw image format

   -.EVE~has case metadata information*(No Answer)*

. EnCase Output Formats

   a. Five Major Categories

   b. ProDiscover Report

   c. **CORRECT:** Types of The Formats ProDiscover Creates

9. -electronically erasable programmable read-only memory

   -how phones store system data

-enables service providers to reprogram phones without having to physically access memory chips

-OS is stored in ROM: nonvolatile memory*(No Answer)*

. Partition

   a. file system

   b. **CORRECT:** EEPROM

   c. SIM Cards

10. -file manipulation: file names and extensions/ hidden property

    -disk manipulation: hidden partitions/bad clusters

    -encryption: bit shifting/stenography*(No Answer)*

. Windows Registry

   a. Examination Plan

   b. Virtual Machine

   c. **CORRECT:** Data-hiding Techniques

11. -gives us a road map to data on a disk

    -type of file system an OS used determines how data is stored on the disk*(No Answer)*

. **CORRECT:** file system

   a. Drive Slack

   b. EEPROM

   c. SIM Cards

12. -the main concerns with mobile devices are loss of power and synchronization with PC's or the cloud (wired or wireless).

    -all mobile devices have volatile memory that may contain valuable information: making sure they don't lose power before you can retrieve RAM data is critical.

    -isolated the device from incoming signals with one of the following options: shielded container (paint can, enclosures), use the Faraday Bag, use eight layers of anti-static bags, aluminum foil.

-if device is not isolated, the data of the device will continue to change while in custody of the specialist.*(No Answer)*

. Additional SIM Card Perposes

a. Network Forensics

b. **CORRECT:** Acquisition Procedures for Mobile Devices

c. Challenges With Mobile Devices

13. -acquisition~preservation~collection

-validation~discrimination~culling

~examination~extraction~review

~reconstruction~analysis

~reporting~presentation~production*(No Answer)*

. Network Forensics

a. **CORRECT:** Five Major Categories

b. SIM Cards

c. Write Blockers

14. -a database that stores hardware and software configuration information, network connections, user preferences, and setup information.

-can contain valuable info about current/past applications and user created information*(No Answer)*

. SIM Cards

a. **CORRECT:** Windows Registry

b. file system

c. Write Blockers

15. -unused space in a cluster between the end of an active file and the end of a cluster. (Includes RAM slack and file slack)*(No Answer)*

. SIM Cards

a. file system

b. Write Blockers

c. **CORRECT:** Drive Slack

16. -subscribers identity module cards

-found most commonly in GSM devices

-microprocessor and from 16KB to 4MB EEPROM

-GSM refers to mobile phones as "mobile station" and divides a station into two parts: the sim card and the mobile equipment and common network in global networks

-portability of information makes SIM cards versatile*(No Answer)*

. EEPROM

a. PDA's

b. **CORRECT:** SIM Cards

c. Drive Slack

17. -EnCase (E01)

-RAW (DD)

-SMART (S01)

-Sleuth Kit (AFF)*(No Answer)*

. Five Major Categories

a. **CORRECT:** Different FTK Output Formats

b. EnCase Output Formats

c. Network Forensics

18. -How long a piece of information lasts on a system versus data that must be collected and preserved before its lost, corrupted, or backed up.

Order:
1-live network devices (switches/routers)
2-live computers/laptops (RAM and processes)
3-live other devices (smartphones, PDA's)

4-Devices/computers already OFF
5-Removable media/cables-adapters/documents*(No Answer)*

. **CORRECT:** Order of Volatility

a. Partition

b. Drive Slack

c. Network Forensics

19. -devices are 'live' computers; traditional "stand-alone OFF computers" approach may be inadequate

-devices are connected to 'live' wireless networks; traditional "disconnect" or "segregate" approach network forensics may be inadequate

-devices lack hardware, software and operating system standardization; many variables affect forensic and eDiscovery techniques and analysis results.

-devices are dynamic in location; communications and operability; computers are mostly static.*(No Answer)*

. **CORRECT:** Challenges With Mobile Devices

a. Write Blockers

b. Network Forensics

c. Acquisition Procedures for Mobile Devices

20. -analog

-digital personal communications service (PC's)

-third-generation (3G and 4G): increased bandwidth

continuing to evolve(No Answer)*

. Data-hiding Techniques

a. **CORRECT:** Three Generations of Mobile Phone Technology

b. Order of Volatility

c. Challenges With Mobile Devices

21. -identifies the subscriber to the network

-stores personal information

-stores address books and messages

-stores service-related information*(No Answer)*

. Five Major Categories

a. ProDiscover Report

b. **CORRECT:** Additional SIM Card Perposes

c. SIM Cards

22. -hardware utilized for protecting source/hard drive from data alteration/tampering while collecting, preserving, and reviewing CSI.

-prevents operating systems and computer programs from making "writes" to the hard drive being acquired, examined, or analyzed.

-write blockers sits between the suspect/source drive and your analysis computer. (It is usually a hardware device, but software based write blockers may be utilized.*(No Answer)*

. file system

a. Drive Slack

b. SIM Cards

c. **CORRECT:** Write Blockers

23. primary Windows based:
-EnCase
-Forensic Tool Kit (FTK)
-ProDiscover
-OSForensics

primarily Linux based:
-Sleuth Kit and Autopsy
-Helix
-Knoppix STD
-SMART*(No Answer)*

. Computer Forensic and EDiscovery Tool Needs

a. **CORRECT:** Computer Forensic Software Tools

b. Network Forensics

c. Mobile Forensics Equiptment

24. -SIM card readers: a combination hardware/software device used to access the SIM card. You need to be in a forensic lap equip with appropriate anti-static devices.

-general forensic procedure for SIM cards:
1-remove the back panel of device
2-remove the battery
3-remove the SIM card
4-insert the SIM card into the card reader
5-extract relevant information

-a variety of SIM card readers are on the market: some are forensically sound and some are not

-documenting messages that haven't been read yet is critical: use a video camera to capture reach screen, if data cannot be extracted with forensic hardware/software

-mobile forensic tools and utilities:
-Ramsey forensic text enclosure (hardware)
-SIM card reader (hardware)
-Paraban Device Seizure (software)
-BitPim (software)
-Susteen SecureView (software)
-EnCase and FTK (software)*(No Answer)*

. file system

a. Network Forensics

b. **CORRECT:** Mobile Forensics Equiptment

c. Computer Forensic Software Tools

25. -EX01

-E01 (Legacy)*(No Answer)*

. **CORRECT:** EnCase Output Formats

a. Different FTK Output Formats

b. EEPROM

c. Network Forensics

26. look for versatility, flexibility, and robustness:
    -Lab OS
    -File System
    -Automated Features
    -Venders Reputation
    -Acceptance by forensic community
    -documented testing and validation

    -Keep in mind what application files and operating system you'd be analyzing*(No Answer)*

. **CORRECT:** Computer Forensic and EDiscovery Tool Needs

a. Mobile Forensics Equiptment

b. Types of The Formats ProDiscover Creates

c. Computer Forensic Software Tools