1.Morris, an attacker, warned to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

wash <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

net view

macof

ntptrace

2.Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

Bluetooth

WPA2-Enterprise

WPA3-Personal <<<<<<<<<<<<<<<<<<<<<<<<

ZigBee

3.George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization betweenindustrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.

What is the short-range wireless communication technology George employed in the above scenario?

LPWAN

MQTT

NB-IoT

Zigbee <<<<<<<<<<<<<<<<<<<<

4.Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. Toaccomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering theorganization's network. Which type of threat intelligence is used by Roma to secure the internal network?

Operational threat intelligence

Strategic threat intelligence

Tactical threat intelligence

Technical threat intelligence <<<<<<<<<<<<<<<<<<<<<<<<<<<<

5.There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of thewireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption. What encryption protocol is being used?

RADIUS

WPA

WEP ,<<<<<<<<<<<<<<<<<<<

WPA3

6.`_____ is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptopor mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.` Fill in the blank with appropriate choice.

Evil Twin Attack <<<<<<<<<<<<<<<<<<<<<<<

Sinkhole Attack

Collision Attack

Signal Jamming Attack

7.As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing. What document describes the specifics of the testing, the associated violations, and essentially protects both the organization’s interest and yourliabilities as a tester?

Service Level Agreement

Project Scope

Rules of Engagement <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Non-Disclosure Agreement

8.Which of these is capable of searching for and locating rogue access points?

NIDS

HIDS

WISS

WIPS ><<<<<<<<<<<<<<<<<<<<<<<<<<<<

9.A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on thenetwork. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

The WAP does not recognize the client's MAC address <<<<<<<<<<<<<<<<<<<<<<<<<<<,

The client cannot see the SSID of the wireless network

Client is configured for the wrong channel

The wireless client is not configured to use DHCP

10.Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from thenetwork operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?

Tap 'n ghost attack

Phishing

Advanced SMS phishing <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Bypass SSL pinning

11.From the following table, identify the wrong answer in terms of Range (ft).

Standard Range (ft)

802.11a 150-150

802.11b 150-150

802.11g 150-150

802.16 (WiMax) 30 miles

802.16 (WiMax)

802.11g

802.11b

802.11a <<<<<<<<<<<<<<<<<<<

12.You want to analyze packets on your wireless network. Which program would you use?

Airsnort with Airpcap

Wireshark with Airpcap <<<<<<<<<<<<<<<<<<<<<<<<,

Wireshark with Winpcap

Ethereal with Winpcap

13.Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

Yagi antenna <<<<<<<<<<<<<<<<<<<<<<<<<

Dipole antenna

Parabolic grid antenna

Omnidirectional antenna

14.Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

Burp Suite

OpenVAS

tshark

Kismet <<<<<<<<<<<<<<<<<<<<<<

15.When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication `open` but sets the SSID to a 32-characterstring of random letters and numbers. What is an accurate assessment of this scenario from a security perspective?

Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.

Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging ג€security through obscurityג€

It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association. <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Javik's router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

16.Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

Bluesmacking

BlueSniffing

Bluejacking <<<<<<<<<<<<<<<<<<<<<<<<<<<

Bluesnarfing

17.An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless dataservices, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol is the most likely able to handle this requirement?

RADIUS <,,,,,,,<<<<<<<<<<<<<<<<<<<<<<<

Kerberos

DIAMETER

TACACS+

18.In an attempt to increase the security of your network, you implement a solution that will help keep your wireless network undiscoverable andaccessible only to those that know it. How do you accomplish this?

Delete the wireless network

Lock all users

Disable SSID broadcasting <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Remove all passwords

19.The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), ratherthan passing only the frames that the controller is intended to receive. Which of the following is being described?

Multi-cast mode

Promiscuous mode <<<<<<<<<<<<<<<<<<<<<<<<

WEM

Port forwarding

20.An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and

exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

Wireshark

Ettercap <<<<<<<<<<<<<<<<

Aircrack-ng

Tcpdump

21.Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a Linux platform?

Kismet <<<<<<<<<<<<<<<<<<<

Abel

Netstumbler

Nessus

22.You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wirelessnetwork with the SSID `Brakeme-Internal.` You realize that this network uses WPA3 encryption. Which of the following vulnerabilities is the promising to exploit?

Cross-site request forgery

Dragonblood <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Key reinstallation attack

AP misconfiguration

23.This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such asGCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

WPA3-Personal

WPA3-Enterprise <<<<<<<<<<<<<<<<<<<<,,

WPA2-Enterprise

WPA2-Personal

24.Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

Wardriving

Wireless sniffing

Evil twin <<<<<<<<<<<<<<<<<<<<<<<<<

Piggybacking

25.A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with theintention to find a free-access wireless network. What is this hacking process known as?

Wardriving <<<<<<<<<<<<<<<<<<<<<<<<

Spectrum analysis

Wireless sniffing

GPS mapping

26.An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue accesspoint with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection wasestablished, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?

Cache-based attack

Timing-based attack

Downgrade security attack ,<<<<<<<<<<<<<<<<<<<<<<

Side-channel attack

27.An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wirelesspassword. What kind of attack is this?

MAC spoofing attack

War driving attack

Phishing attack

Evil-twin attack <<<<<<<<<<<<<<<<<<<<<<

28.The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneousauthentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept. What is the Wi-Fi encryption technology implemented by Debry Inc.?

WPA

WEP

WPA3 <<<<<<<<<<<<<<<<<<<<<<

WPA2

29.Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in thenetwork, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

LNMIB2.MIB <<<<<<<<<<<<<<<<<<<<<<,

DHCP.MIB

MIB_II.MIB

WINS.MIB

30.Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, andimprove defense strategies against attacks. What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

Reverse engineering <<<<<<<<<<<<<<<<<<<

App sandboxing

Jailbreaking

Social engineering

31.Which of the following is the best countermeasure to encrypting ransomwares?

Use multiple antivirus softwares

Pay a ransom

Keep some generation of off-line backup <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Analyze the ransomware to get decryption key of encrypted data

32.Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone werereplaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app. What is the attack performed on Don in the above scenario?

SIM card attack

Clickjacking

SMS phishing attack

Agent Smith attack <<<<<<<<<<<<<<<<<<<<<<<<<

33.What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

AndroidManifest.xml ,<<<<<<<<<<<<<<<<<<<<<<

classes.dex

APK.info

resources.asrc

34.Which of the following is not a Bluetooth attack?

Bluedriving <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Bluesmacking

Bluejacking

Bluesnarfing

35.A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing `” Reports

https://ibt1.prometric.com/users/custom/report_queue/rq_str… corporate network. What tool should the analyst use to perform a Blackjacking attack?

Paros Proxy

BBProxy <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Blooover

BBCrack

36.Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the publiccomputer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, evenafter the device is out of the communication zone. Which of the following attacks is performed by Clark in the above scenario?

Man-in-the-disk attack

iOS jailbreaking

iOS trustjacking <<<<<<<<<<<<<<<<<<<<<<<<<<<

Exploiting SS7 vulnerability

37.Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the targetmobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

DroidSheep

Androrat

Trident <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Zscaler

38.Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attackallowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?

btlejack -f 0x9c68fd30 -t -m 0x1fffffffff <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

btlejack -c any

btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

btlejack -f 0x129f3244 -j

39.Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy. What is the type of attack Bob performed on Kate in the above scenario?

SIM card attack

aLTEr attack

Spearphone attack <<<<<<<<<<<<<<<<<<<<<<<<<<<

Man-in-the-disk attack

40.What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

White-hat hacking program

Bug bounty program <<<<<<<<<<<<<<<<<<<<<<<<<<<

Ethical hacking program

Vulnerability hunting program

41.Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock networkused for delivering a synchronized signal across the chip. Which of the following types of fault injection attack is performed by Robert in the above scenario?

Frequency/voltage tampering

Optical, electromagnetic fault injection (EMFI)

Temperature attack

Power/clock/reset glitching <<<<<<<<<<<<<<<<<<<<<<<<<<<<<

42.Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, hestarted injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices. What is the type of attack performed by Richard in the above scenario?

Cryptanalysis attack

Reconnaissance attack

Side-channel attack

Replay attack <<<<<<<<<<<<<<<<<<<<<<<<

43.Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

Bluesmacking

Bluesnarfing <<<<<<<<<<<<<<<<<<<<<<<<<<

Bluejacking

Bluebugging

44.Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoTdevice and the certifications granted to it. Which of the following tools did Bob employ to gather the above information?

FCC ID search <<<<<<<<<<<<<<<<<<<<

Google image search

search.com

EarthExplorer

45.What is the role of test automation in security testing?

It is an option but it tends to be very expensive.

It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

Test automation is not usable in security due to the complexity of the tests.

It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely. <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<,,,,,,

46.Mirai malware targets IoT devices.

After infiltration, it uses them to propagate and create botnets that are then used to launch which types of attack?

MITM attack

Password attack

Birthday attack

DDoS attack <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

47.What is the port to block first in case you are suspicious that an IoT device has been compromised?

22

48101 <<<<<<<<<<<<

80

48.Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device onthe Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

NeuVector

Lacework

Censys <<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Wapiti

49.John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are usingdefault credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?

IoT Inspector

AT&T IoT Platform

IoT Seeker <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Azure IoT Central

50.Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulatingcommunication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level virtualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?

Virtual machine

Docker <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Zero trust network

Serverless computing

51.According to the NIST cloud deployment reference architecture, which of the following provides connectivity and transport services to consumers?

Cloud connector

Cloud broker

Cloud carrier <<<<<<<<<<<<<<

Cloud provider

52.Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloudservice provider. In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

Cloud consumer

Cloud broker

Cloud auditor

Cloud carrier <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

53.Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of thecloud-based resources. Which of the following models covers this?

Platform as a service

Software as a service

Functions as a service

Infrastructure as a service <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

54.There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group ofusers or organizations to share a cloud environment. What is this cloud deployment option called?

Private

Community <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Public

Hybrid

55.Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided topurchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

IaaS

SaaS <<<<<<<<<<<<<<<<<<<<<<<<<<

PaaS

CaaS

56.Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP. What part of the contract might prevent him from doing so?

Lock-down

Virtualization

Lock-in <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Lock-up

57.Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emailsand distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

Cloud cryptojacking

Man-in-the-cloud (MITC) attack

Cloud hopper attack <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Cloudborne attack

58.What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

White-hat hacking program

Bug bounty program <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Ethical hacking program

Vulnerability hunting program

59.Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability ina bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS. What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

Cloudborne attack <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Man-in-the-cloud (MITC) attack

Metadata spoofing attack

Cloud cryptojacking

60.Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes acomponent that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

Docker objects

Docker daemon <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Docker client

Docker registries

61.Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization ofapplications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture is Abel currently working in?

Tier-1: Developer machines

Tier-2: Testing and accreditation systems <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Tier-3: Registries

Tier-4: Orchestrators

62.Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a nodeto them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions. Which of the following master components is explained in the above scenario?

Kube-apiserver

Etcd cluster

Kube-controller-manager

Kube-scheduler <<<<<<<<<<<<<<<<<<<<<<<<<<<<<

63.Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access tothe network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role. What is the technique employed by Eric to secure cloud resources?

Demilitarized zone

Zero trust network <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Serverless computing

Container technology

64.Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using thistechnique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks. What is the technique employed by Kevin to improve the security of encryption keys?

Key stretching <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Public key infrastructure

Key derivation function

Key reinstallation

65.BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might losetheir cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?

Key archival

Certificate rollover

Key escrow <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Key renewal

66.Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Samused an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

PGP

SMTP

GPG <<<<<<<<<<<<<<<<<<<<<<<<<<<<

S/MIME

67.Bill has been hired as a penetration tester and cyber security auditor for a major credit card company. Which information security standard is most applicable to his role?

FISMA

Sarbanes-Oxley Act

HITECH

PCI-DSS <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

68.Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 — 32-bit S-boxes(S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key (Km1) and a rotation key (Kr1) for performing its functions. What is the algorithm employed by Harper to secure the email messages?

CAST-128 <<<<<<<<<<<<<<<<<<<<<<<<<<<<

AES

GOST block cipher

DES

69.PGP, SSL, and IKE are all examples of which type of cryptography?

Digest

Secret Key

Public Key <<<<<<<<<<<<<<<<<<<<<<<<<<<<

Hash Algorithm

70.In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

Evil twin

Chop chop attack

Wardriving

KRACK <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

71.Which of the following protocols can be used to secure an LDAP service against anonymous queries?

NTLM <<<<<<<<<<<<<<<<<<<<<<<<

RADIUS

WPA

SSO

72.Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the messageusing their private key. What is the security model implemented by Jane to secure corporate messages?

Zero trust network

Secure Socket Layer (SSL)

Transport Layer Security (TLS)

Web of trust (WOT) <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

73.Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address thissituation, Bella implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols is used by Bella?

FTPS <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

FTP

HTTPS

IP

74.What is correct about digital signatures?

A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Digital signatures may be used in different documents of the same type.

A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.

Digital signatures are issued once for each user and can be used everywhere until they expire.

75.Alice needs to send a confidential document to her coworker, Bryan. Their company has public key infrastructure set up. Therefore, Alice both encrypts the message and digitally signs it. Alice uses _____ to encrypt the message, and Bryan uses _____ to confirm the digital signature.

Bryan's public key; Bryan's public key

Alice's public key; Alice's public key

Bryan's private key; Alice's public key

Bryan's public key; Alice's public key <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

76.Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 roundsof computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

CAST-128

RC5

TEA

Serpent <<<<<<<<<<<<<<<<<<<<<<<<<<<

77.What two conditions must a digital signature meet?

Has to be the same number of characters as a physical signature and must be unique.

Has to be unforgeable, and has to be authentic. <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Must be unique and have special characters.

Has to be legible and neat.

78.What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

CPU

UEFI

GPU

TPM <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

79.In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

IDEA

Triple Data Encryption Standard <<<<<<<<<<<<<<<<<<<<<<<<<

AES

MD5 encryption algorithm

80.Which of the following is assured by the use of a hash?

Authentication

Confidentiality

Availability

Integrity <<<<<<<<<<<<<<<<<<<<<<<<<<<

81.John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives himthe idea of using PGP. What should John do to communicate correctly using this type of encryption?

Use his own private key to encrypt the message.

Use his own public key to encrypt the message.

Use Marie's private key to encrypt the message.

Use Marie's public key to encrypt the message. <<<<<<<<<<<<<<<<<<<<<<<<<<<<<

82.This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

HMAC encryption algorithm

Twofish encryption algorithm <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

IDEA

Blowfish encryption algorithm

83.This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such asGCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

WPA3-Personal

WPA3-Enterprise <<<<<<<<<<<<<<<<<

WPA2-Enterprise

WPA2-Personal

84.Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.

Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key. <<<<<<<<<<<<<<<<<<<<<<<<

Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

85.User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

Application

Transport

Session

Presentation <<<<<<<<<<<<<<<<<<<<<,,,,,,,,

86.Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

SOA

biometrics

single sign on

PKI <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

87.What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.

Symmetric encryption allows the server to security transmit the session keys out-of-band.

Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography. <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

88.What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

Man-in-the-middle attack

Meet-in-the-middle attack <<<<<<<<<<<<<<<<<<<<<<<<<

Replay attack

Traffic analysis attack

89.In the field of cryptanalysis, what is meant by a `rubber-hose` attack?

Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.

A backdoor placed into a cryptographic algorithm by its creator.

Extraction of cryptographic secrets through coercion or torture. ><<<<<<<<<<<<<<<<<<<<

Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

90.The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statementsneed to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

The CFO can use a hash algorithm in the document once he approved the financial statements
<<<<<<<<<<<<<<<<<<<<<<

The CFO can use an excel file with a password

The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure isthe same document

The document can be sent to the accountant using an exclusive USB for that document

91.What is a `Collision attack` in cryptography?

Collision attacks try to get the public key

Collision attacks try to break the hash into three parts to get the plaintext value

Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

Collision attacks try to find two inputs producing the same hash
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

92.A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?

Man-in-the-middle attack

Brute-force attack

Dictionary attack <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Session hijacking

93.During the process of encryption and decryption, what keys are shared?

Public keys <<<<<<<<<<<<<<<<<<<<<<<<

Private keys

Public and private keys

User passwords

94.How can rainbow tables be defeated?

Use of non-dictionary words

All uppercase character passwords

Password salting <<<<<<<<<<<<<<<<<<<<<<<

Lockout accounts under brute force password cracking attempts

95.Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts itusing asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?

Alice's public key

His own public key

His own private key <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Alice's private key

96.Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

Full Disk encryption <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

BIOS password

Hidden folders

Password protected files