Alison is examining a digital certificate presented to her by her bank's website. Which one of the following requirements is not necessary for her to trust the digital certificate?

She knows that the server belongs to the bank.

James has opted to implement a NAC solution that uses a post-admission philosophy for its control of network connectivity. What type of issues can't a strictly post-admission policy handle?

Preventing an unpatched laptop from being exploited immediately after connecting to the network

When Mike receives Renee's digital certificate, what key does he use to verify the authenticity of the certificate?

CA's private key

Renee's private key

Renee's public key

CA's public key

CA's public key

Which of the following would best describe secondary evidence?

Evidence that proves a specific act

Oral testimony by an expert witness

A copy of a piece of evidence

Oral testimony by a non-expert witness

A copy of a piece of evidence

Patching a system, ending a process, rebooting a system, quarantine a virus are all technical controls that are:

Control Type: Physical, Technical, Administrative

Control Function: Preventative, Detective, Corrective

Technical, Corrective

CCTV, Surveillance cameras, and logs are examples of:

Control Type: Physical, Technical, Administrative

Control Function: Preventative, Detective, Corrective

Physical, Detective

Policies, separations of duties, classifications are examples of:

Control Type: Physical, Technical, Administrative

Control Function: Preventative, Detective, Corrective

Administrative, Preventative

Tommy handles access control requests for his organization. A user approaches him and explains that he needs access to the human resources database to complete a headcount analysis requested by the CFO. What has the user demonstrated successfully to Tommy?

Clearance

Separation of duties

Need to know

Isolation

Need to know

His supervisor (who is on holiday leave) has apparently logged on remotely, used remote desktop features to take control of Pedro's system, and is trying to dump huge amounts of chemicals into the water being treated.

Customer's storage team

Customer's security team

Vendor

Vendor

Chris needs to design a firewall architecture that can support a DMZ, a database, and a private internal network in a secure manner that separates each function. What type of design should he use, and how many firewalls does he need? (DMZ, Database, and Priv-Net) = 3 tiers.

A three-tier firewall design with at least one firewall

A two-tier firewall design with three firewalls

A four-tier firewall design with two firewalls

A single-tier firewall design with three firewalls

A three-tier firewall design with at least one firewall

What is the final step of a quantitative risk analysis?

Assess the annualized rate of occurrence.

Determine asset value.

Conduct a cost/benefit analysis.

Derive the annualized loss expectancy.

Conduct a cost/benefit analysis.

Decomposition

Static analysis

Composition

Decomposition

Lauren’s organization has deployed VoIP phones on the same switches that the desktop PCs are on. What security issue could this create, and what solution would help?

Denial-of-service attacks; use a firewall between networks.

VLAN hopping; use physically separate switches.

Caller ID spoofing; MAC filtering

VLAN hopping; use encryption.

VLAN hopping; use physically separate switches.

Which of the following would be LESS likely to prevent an employee from reporting an incident?

They are afraid of being pulled into something they don't want to be involved with.

The process of reporting incidents is centralized.

They are afraid of being accused of something they didn't do.

SOC 2

SOC 1

SOC 2

What layer of the OSI model is associated with datagrams?

Network

Transport

Session

Data Link

Transport - Datagrams

Carla has worked for her company for 15 years and has held a variety of different positions. Each time she changed positions, she gained new privileges associated with that position, but no privileges were ever taken away. What concept describes the sets of privileges she has accumulated?

Entitlement

Aggregation

Transitivity

Isolation

Checklist review

Chris would like to use John the Ripper to test the security of passwords on a compromised Linux system. What files does he need to conduct this analysis?

/etc/user and /etc/account

/etc/shadow and /etc/user

/etc/passwd and /etc/shadow

/etc/passwd and /etc/user

/etc/passwd and /etc/shadow

What type of fire extinguisher is useful against liquid-based fires?

Class A

Class B

Class C

Class D

Class B

A-Dry

B-Wet

C-Electrical

D-Metals

If Susan’s organization requires her to log in with her username, a PIN, a password, and a retina scan, how many distinct authentication factor types has she used?

One

Three

Two

Four

Two -Something she knows, something you are

Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric).

An administrator wants to install a system on an e-mail server with the goal of preventing attacks. Which of the following would be most suitable for that purpose?

HIDS

NIDS

HIPS

NIPS

Due care - keep in working order.

A company wants to select a dedicated alternative location for continuing its operations in the event of an incident, while minimizing operational downtime. Which of the following would be most appropriate for that purpose?

Cold site

Warm site

Mobile site

Hot site

Hot Site

Darcy is a computer security specialist who is assisting with the prosecution of a hacker. The prosecutor requests that Darcy give testimony in court about whether, in her opinion, the logs and other records in a case are indicative of a hacking attempt. What type of evidence is Darcy being asked to provide?

Documentary evidence

Real evidence

Direct evidence

Expert opinion

Expert opinion

MAC

T or F: Tim needs to lock down a Windows workstation that has recently been scanned using nmap with the results shown here. He knows that the workstation needs to access websites and that the system is part of a Windows domain. No ports should be open!

True

Which of the following strategies is not a reasonable approach for remediating a vulnerability identified by a vulnerability scanner?

Install a patch.

Update the banner or version number.

Use an application layer firewall or IPS to prevent attacks against the identified vulnerability.

Use a workaround fix.

Update the banner or version number.

Which authentication technique best protects against hijacking?

Continuous authentication

Static authentication

Robust authentication

Strong authentication

Continuous authentication

Susan would like to configure IPsec in a manner that provides confidentiality for the content of packets. What component of IPsec provides this capability?

ISAKMP

AH

IKE

ESP

ESP

Which of the following steps should be one of the first step performed in a Business Impact Analysis (BIA)?

Estimate the Recovery Time Objectives (RTO).

Identify and Prioritize Critical Organization Functions

Identify all CRITICAL business units within the organization.

Evaluate the impact of disruptive events

Identify all CRITICAL business units within the organization.

Unique salts should be stored for each user.

Unique salts should be created every time a user logs in.

A single salt should be set so passwords can be de-hashed as needed.

A single salt should be used so the original salt can be used to check passwords against their hash.

Unique salts should be stored for each user.

Saria's team is working to persuade their management that their network has extensive vulnerabilities that attackers could exploit. If she wants to conduct a realistic attack as part of a penetration test, what type of penetration test should she conduct?

Crystal box

Gray box

White box

Black box

Black Box

Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?

Basement

Third floor

The programmer should not be allowed to work on security software. The remaining roles have valid reasons.

What type of key does WEP use to encrypt wireless communications?

A predefined shared static key

An asymmetric key

Unique asymmetric keys for each host

Unique key sets for each host

A predefined shared static key

What type of virus is characterized by the use of two or more different propagation mechanisms to improve its likelihood of spreading between systems?

Polymorphic virus

Stealth virus

Multipartite virus

Encrypted virus

Multipartite virus