Which type of control should be implemented to prevent future spear phishing attacks?

A Mutual authentication

B Strong passwords

C Employee training

D Input validation - ***CORRECT ANSWER***-C

A company has instituted a policy to prevent data leakage. The policy requires that any data stored on USB storage devices must be encrypted with at least 256-bit encryption.

Which principle that is part of the Parkerian hexad but not the CIA triad would be violated if one of these devices was stolen?

A Confidentiality

B Integrity

C Possession

D Authenticity - ***CORRECT ANSWER***-C

A company is concerned about potential phishing attacks through email. As a result, a new company policy dictates that all email must be digitally signed before it is sent to any customers or partners.

Which security principle that is part of Parkerian hexad but not part of the CIA triad is precipitating this policy change?

A Confidentiality

B Authenticity

C Control

D Utility - ***CORRECT ANSWER***-B

Which two principles of the CIA triad can be violated by a fabrication attack?

A Integrity and authenticity

B Integrity and availability

C Confidentiality and integrity

D Confidentiality and availability - ***CORRECT ANSWER***-B

Which two principles of the CIA triad can be violated by an interruption attack?

A Confidentiality and availability

B Confidentiality and integrity

C Integrity and availability

D Integrity and authenticity - ***CORRECT ANSWER***-C

Which attack category targets the confidentiality of data?

A Interruption

B Modification

C Interception

D Fabrication - ***CORRECT ANSWER***-C

A bank website accepts online loan applications. It requires applicants to review and sign a disclosure document explaining the organization's information sharing practices.

Which federal law protects consumer's financial information?

A SOX

B GLBA

C FERPA

D HIPAA - ***CORRECT ANSWER***-B

A retail store has hired a third party to audit its computer and network systems that process credit card payments.

Which industry standard is the retail store addressing?

A FERPA

B HIPAA

C SOX

D PCI DSS - ***CORRECT ANSWER***-D

In order to continue processing credit card payments, a retail store arranges for an external auditor to perform regular external and internal vulnerability scans.

Which regulation are they addressing?

A GLBA

B PCI DSS

C FCRA

D HIPAA - ***CORRECT ANSWER***-B

A hospital allows its patients to pay by credit card.

Which set of regulations apply to the hospital's operations?

A HIPAA and FCRA

B FERPA and PCI DSS

C HIPAA and PCI DSS

D FERPA and HITECH - ***CORRECT ANSWER***-C

While visiting a country in the European Union, an American purchases an expensive bottle of perfume with a credit card.

What does the European Union Directive 95/46/EC regulation safeguard for the purchaser?

Your organization's network was recently the target of an attack. Fortunately, the new system you installed took action and refused traffic from the source before you even had a chance to respond. What system did you install?

A An authorization system

B An intrusion detection system

C A logging system

D An intrusion prevention system

E An authentication system - ***CORRECT ANSWER***-D

A surveillance video log contains a record, including the exact date and time, of an individual gaining access to his company's office building after hours. He denies that he was there during that time, but the existence of the video log proves otherwise. What benefit of accountability does this example demonstrate?

A Authorization

B Deterrence

C Nonrepudiation

D Intrusion detection and prevention

E Authentication - ***CORRECT ANSWER***-C

What process ensures compliance with applicable laws, policies, and other bodies of administrative control, and detects misuse?

A Deterrence

B Nonrepudiation

C Authorization

D Accountability

E Auditing - ***CORRECT ANSWER***-E

_____ provides us with the means to trace activities in our environment back to their source.

A Accountability

D Vulnerabilities

E Scanners - ***CORRECT ANSWER***-B

Which software development vulnerability occurs when multiple processes control or share access to a particular resource, and the correct handling of that resource depends on the proper ordering or timing of transactions?

A Authentication attacks

B Input validation attacks

C Race conditions

D Buffer overflows

E Authorization attacks - ***CORRECT ANSWER***-C

Which Microsoft fuzzing tool examines source code for general good practices?

A MiniFuzz File Fuzzer

B BinScope Binary Analyzer

C Nessus

D Nikto/Wikto

E Burp Suite - ***CORRECT ANSWER***-B

Which tool performs checks for many common server-side vulnerabilities, and creates an index of all the files and directories it can see on the target Web server?

A MiniFuzz File Fuzzer

B BinScope Binary Analyzer

C Nessus

D Nikto/Wikto

E NetStumbler - ***CORRECT ANSWER***-D

Which of the following is not a major category of database security issues?

Spoofing emails is an example of _____. - ***CORRECT ANSWER***-Fabrication

Eavesdropping on a phone is an example of _____. - ***CORRECT ANSWER***-Interception

DDoS on a mail server is an example of _____. - ***CORRECT ANSWER***-Interruption

Altering a web server config file is an example of _____. - ***CORRECT ANSWER***-Modification

The likelihood that something bad will happen. - ***CORRECT ANSWER***-Risk

Weaknesses that can be used to harm us. - ***CORRECT ANSWER***-Vulnerabilities

Something that has the potential to cause us harm. - ***CORRECT ANSWER***-Threat

The value of the asset is used to assess if a risk is present. - ***CORRECT ANSWER***-Impact

The first most important part of the risk management process is_____. - ***CORRECT ANSWER***-Identifying and Categorizing Assets

_____controls, are those that protect the systems, networks, and environments that process, transmit, and store our data. Common examples are: passwords, encryption, logical access controls, firewalls, and intrusion detection systems. - ***CORRECT ANSWER***-Logical and Technical Controls

_____ are based on rules, laws, policies, procedures, guidelines, and other items that are "paper" in nature. An example is one that requires us to change our password every 90 days. One important concept when we discuss this type of control is the ability to enforce compliance with them. If we do not have the authority or the ability to ensure that our controls are being complied with, they are worse than useless, because they create a false sense of security. - ***CORRECT ANSWER***-Administrative Controls

A tool used to detect unauthorized wireless access points. - ***CORRECT ANSWER***-Kismet

A versatile tool able to scan ports, search for hosts on the network, and other operations. - ***CORRECT ANSWER***-Nmap

This command-line packet sniffing tool runs on Linux and UNIX operating systems. - ***CORRECT ANSWER***-Tcpdump

A graphical interface protocol analyzer capable of filtering, sorting, and analyzing both wired and wireless network traffic. - ***CORRECT ANSWER***-Wireshark

1 - Removing unnecessary software

2 - Removing or turning off unessential services

3 - Making alterations to common accounts

4 - Applying the principle of least privilege

5 - Applying software updates in a timely manner

6 - Making use of logging and auditing functions

7 - Remove All Unnecessary Software - ***CORRECT ANSWER***-Operating System Hardening (Steps)

This type of host-based software may communicate with the management device by sending regular beacons.

A Malware signature

B HIDS

C Software firewall

D Buffer overflow - ***CORRECT ANSWER***-B

A category of tools, or more accurately, a category of sets of tools, called an _____. - ***CORRECT ANSWER***-Exploit Framework

Metasploit