5-2

Study online at https://quizlet.com/_fhygwr

An ethical hacker has been hired to conduct a physical penetration test of a company. During the first day of the test, the ethical hacker dresses up like a plumber and waits in the main lobby of the building until an employee goes through the main turnstile. As soon as the employee enters his access number and proceeds to go through the turnstile, the ethical hacker follows them through the access gate. What type of attack did the ethical hacker utilize to access the restricted area of the building? • Tailgating • Mantrap • Shoulder surfing • Social engineering	Tailgating Explanation OBJ-1.2: The ethical hacker is conducting a very specialized type of social engineering attack known as tailgating. Sometimes on a certification exam, there are two correct answers, but one is more correct. This question is an example of that concept. Tailgating involves someone who lacks the proper authentication following an employee into a restricted area. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder.
You are notified by an external organization that an IP address associated with your company's email server has been sending spam emails requesting funds as part of a lottery collection scam. An investigation into the incident reveals the email account used was Connor from the sales department, and that Connor's email account was only used from one workstation. You analyze Connor's workstation and discover several unknown processes running, but netflow analysis reveals no attempted lateral movement to other workstations on the network. Which containment strategy would be most effective to use in this scenario? • Isolate the network segment Connor is on and conduct a forensic review of all workstations in the sales department • Isolate the workstation computer by disabling the switch port and reset Connor's username/password • Request disciplinary action for Connor for causing this incident • Unplug the workstatio	Isolate the workstation computer by disabling the switch port and reset Connor's username/password Explanation OBJ-3.2: Isolation of Connor's computer by deactivating the port on the switch should be performed instead of just unplugging the computer. This would guarantee that Connor won't just plug the computer back into the network as soon as you leave his desk. While Connor won't be able to work without his workstation, it is essential to isolate the issue quickly to prevent future attempts at lateral movement from occurring and protecting the company's data that is needed for continued business operations. While we are unsure of the initial root cause of the issue, we know it is currently isolated to Connor's machine. He should receive remedial cybersecurity training, his workstation's hard drive forensically imaged for later analysis, and then his workstation should be remediated or reimaged. It is better to isolate just Connor's machine instead of the entire network segment in this scenario. Isolating the network segment, without evidence indicating the need to do so, would have been overkill and overly disruptive to the business. Reimaging Connor's device may destroy data that could have otherwise been recovered and led to a successful root cause analysis. There is also insufficient evidence in this scenario to warrant disciplinary action against Connor as he may have simply clicked on a malicious link by mistake.
Which of the following access control methods provides the most detailed and explicit type of access control over a resource? • DAC • MAC • ABAC • RBAC	ABAC Explanation OBJ-4.3: Attribute-based access control (ABAC) provides the most detailed and explicit type of access control over a resource because it is capable of making access decisions based on a combination of subject and object attributes, as well as context-sensitive or system-wide attributes. Information such as the group membership, the OS being used by the user, and even the IP address of the machine could be considered when granting or denying access.
Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices? • Installation of anti-virus tools • Implement endpoint protection platforms	User and entity behavior analytics Explanation OBJ-3.5: Since ICS, SCADA, and IoT devices often run proprietary, inaccessible, or unpatchable operating systems, the traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly. Therefore, the use of user and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline. Once a known-good baseline is established, deviations can be detected and analyzed. UEBA may be heavily

• Use of a host-based IDS or IPS • User and entity behavior analytics	dependent on advanced computing techniques like artificial intelligence and machine learning, and may have a higher false positive rate. As the name suggests, the analytics software tracks user account behavior across different devices and cloud services. Entity refers to machine accounts, such as client workstations or virtualized server instances, and to embedded hardware, such as Internet of Things (IoT) devices. Traditional technologies include anti-virus tools, host-based IDS and IPS, and endpoint protection platforms.
Which mobile device strategy is most likely to result in the introduction of vulnerable devices to a corporate network? • BYOD • COPE • MDM • CYOD	BYOD Explanation OBJ-2.5: The BYOD (bring your own device) strategy opens a network to many vulnerabilities. People are able to bring their personal devices to the corporate network, and their devices may contain vulnerabilities that could be allowed to roam free on a corporate network. COPE (company-owned/personally enabled) means that the company provides the users with a smartphone primarily for work use, but basic functions such as voice calls, messaging, and personal applications are allowed, with some controls on usage and flexibility. With CYOD, the user can choose which device they wish to use from a small selection of devices approved by the company. The company then buys, procures, and secures the device for the user. The MDM is a mobile device management system that gives centralized control over COPE company-owned personally enabled devices.
You need to determine the best way to test operating system patches in a lab environment prior to deploying them to your automated patch management system. Unfortunately, your network has several different operating systems in use, but you only have one machine available to test the patches on. What is the best environment to utilize to perform the testing of the patches prior to deployment? • Sandboxing • Purchase additional workstations • Bypass testing and deploy patches directly into the production environment • Virtualization	Virtualization Explanation OBJ-3.3: When you have a limited amount of hardware resources to utilized but have a required to test multiple operating systems, you should set up a virtualized environment to test the patch across each operating system prior to deployment. You should never deploy patches directly into production without testing them first in the lab.
(Sample Simulation - On the real exam for this type of question, you would receive 3-5 pictures and be asked to drag and drop them into place next to the correct term.) Larger image How would you appropriately categorize the authentication method being displayed here? • One-time password authentication • Biometric authentication • Multi-factor authentication • PAP authentication	PAP authentication Explanation OBJ 4.1: For the exam, you need to know the different categories of authentication and what type of authentication methods belong to each category. A username and password is used as part of the Password Authentication Protocol (PAP) authentication system. A username and password is also considered a knowledge factor in an authentication system.
Which of the following is the leading cause for cross-site scripting, SQL injection, and XML injection attacks? • File inclusions • Faulty input validation • Directory traversals • Output encoding	Faulty input validation Explanation OBJ-3.6: A primary vector for attacking applications is to exploit faulty input validation. The input could include user data entered into a form or URL, passed by another application or link. This is heavily exploited by cross-site scripting, SQL injection, and XML injection attacks. Directory traversal is the practice of accessing a file from a location that the user is unauthorized to access. The attacker does this by ordering an application to backtrack through the directory path so that the application reads or executes a file in a parent directory. In a file inclusion attack, the attacker adds a file to the running process of a web app or website. The file is either

	constructed to be malicious or manipulated to serve the attacker's malicious purposes. Cross-site scripting (XSS) is one of the most powerful input validation exploits. XSS involves a trusted site, a client browsing the trusted site, and the attacker's site.
Tony works for a company as a cybersecurity analyst. His company runs a website that allows public postings. Recently, users have started complaining about the website having pop-up messages asking for their username and password. Simultaneously, your security team has noticed there has been a large increase in the number of compromised user accounts on the system. What type of attack is most likely the cause of both of these events? • Cross-site scripting • Cross-site request forgery • SQL injection • Rootkit	Cross-site scripting Explanation OBJ-1.2: This scenario is a perfect example of the effects of a cross-site scripting (XSS) attack. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, then an attacker can create a pop-up window that collects passwords and uses that information to further compromise other accounts. A cross-site request forgery (CSRF) is an attack that forces an end-user to execute unwanted actions on a web application in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the browser of a victim user (such as creating pop-ups). A CSRF would allow an attack to induce a victim to perform actions that they do not intend to perform. A rootkit is a set of software tools that enable an unauthorized user to gain control of a computer system without being detected. SQL injection is the placement of malicious code in SQL statements, via web page input. None of the things described in this scenario would indicate a CSRF, rootkit, or an SQL injection.