Compensating controls are used to fulfill the same objective control as required control when it is not feasible to implement that required control. The scenario describes a need for a compensating control. This control may be technical, operational, and / or administrative in nature.

Zero - day exploits take advantage of a security vulnerability that is not known until the exploit has been used - there is no time (zero days) between the discovery and the attack.

Threat hunting activities presume that a compromise has already taken place and search for indicators of that compromise. Vulnerability scanning activities probe systems for known vulnerabilities. The user's activity could be described as intrusion detection, but not as intrusion prevention because he is not taking any action to block future attacks. Data mining is a generic term used in machine learning activities and the user is not leveraging data mining in this work.

Honeypots are decoy systems used to attract the attention of intruders so that they may be monitored in a controlled environment. Mandatory access controls (MACs) are used to enforce system security policies. Intrusion prevention systems are designed to detect and block malicious activity. Rogue access points provide an unauthorized means of wireless access.

This is an example of delivering the payload to the victim, so it is from the Delivery stage of the Cyber Kill Chain.

A jump box is a system designed to accept remote connection requests and act as an intermediary between those remote systems and local hosts. Virtual machines, honeypots, and firewalls may all exist in the DMZ but do not have the express purpose of providing remote administrative access.

Port 1433 is used for Microsoft SQL Server and should not be exposed on a web server. Ports 22, 80, and 443 are required for SSH, HTTP, and HTTPS connectivity, respectively.

Sampling is often used to retain flow visibility while reducing the overall flow rates to a reasonable level. Rates of 1:10, 1: 100, or 1: 1000 can significantly decrease the load that flows create while providing useful visibility. RMON does not provide visibility into flow data. Decreasing the number of flows per user would require reducing users' ability to use the network, much like using packet shaping to reduce traffic rates would cause the network to be less usable - not a desirable option in almost any network!

Infrastructure as a service (IaaS) is the only cloud service model where customers would configure operating systems themselves. In platform as a service (PaaS), function as a service (Faas), and software as a service (SaaS) models, the cloud service provider is responsible for an operating system configuration.

This is an example of a captive portal network access control (NAC) solution, which is an in - band NAC because it inserts a device between the user and the Internet. Out - of - band solutions, such as 802.1x, require that the user's system communicate with the network switch to support NAC. Agent - based solutions would require the installation of software on the user's computer.

A network access control (NAC) system can allow the user to require network authentication while performing security posture assessments on the systems that connect. This will allow his team to authenticate and use the network if they have secure systems.

The Trusted Platform Module (TPM) is a hardware chip found inside most modern computers that is used to store disk encryption keys. Hardware security modules (HSMs) also store encryption keys, but they are dedicated, costly devices. Trusted foundries are trusted sources for I hardware, and the root of trust is a concept used to describe how trust flows through the components of a secure system.

I Destruction is both the most effective and the costliest option identified in the NIST Guidelines for Media Sanitization. Clearing by using logical methods to clear addressable storage locations and using overwriting and cryptographic erase techniques for purging are both cheaper and easier to perform. Obliteration is not an option in the NIST listing.

Next - generation firewalls (NGFWs) are able to incorporate contextual information about a connection attempt when making access control decisions. This capability is not available in packet filters or stateful inspection firewalls. While an NGFW may be a perimeter firewall, not all perimeter firewalls have next-generation capabilities.

During a network attack simulation, the blue team is responsible for securing the targeted environment and keeping the attacking (red) team out. The white team serves as referees. There is no black team during a network attack simulation,

the three pillars of information security are confidentiality, integrity, and availability. Attacks against confidentiality seek to disclose sensitive information. Attacks against integrity seek to alter information in an unauthorized manner. Attacks against availability seek to prevent legitimate use of information or systems.

Segmentation occurs in the containment phase in the CompTIA incident response process. Bear in mind that CompTIA's incident response process differs from the NIST standard, and places sanitization, reconstruction / re-imaging, and secure disposal in the eradication and recovery phase.

Environmental threats are natural or man - made disasters outside the control of the organization. Accidental threats occur when an inadvertent action jeopardizes security. Adversarial threats occur when someone is actively seeking to attack the organization. Structural threats occur when there is an exhaustion of available resources, PCI DSS is an information security standard required by major payment card brands for organizations that use their cards. HIPAA, SOX, and FERPA are all U.S.A. laws.

For most organizations, CSIRT activities initially involve internal resources. Law enforcement is involved only whertit is believed that a crime has been committed, requiring participation of law enforcement officers.

Network reconnaissance normally takes place during the discovery phase of a penetration test. The attack phase consists of gaining access, escalating privileges, system browsing, and installing additional tools.

Under the risk management matrix used by most organizations, a risk with a medium likelihood and high impact would be considered a high risk.

Bandwidth consumption, beaconing, and unexpected traffic are all common network issues that you should monitor for. Link aggregation refers to combining links to create a higher throughput link.

Distributed denial - of - service (DDoS) attacks can be detected in many ways, including use of SIEM devices, IDSs and IPSs, network bandwidth and connection monitoring tools, and performance monitoring utilities. Fuzzers are used to send unexpected data to applications and won't help detect a DDoS.

Application programming interfaces (APIs) are used to programmatically integrate systems, including SaaS platforms. Security orchestration, automation, and response (SOAR) does integrate systems but specifically in the security, not productivity, space. The Security Content Automation Protocol (SCAP) also is used to integrate security, not productivity, systems. Continuous integration / continuous delivery (C1 / CD) is an operational philosophy and not a specific technology

Although the bandwidth used for active monitoring is typically relatively low, it does add to the total network load traffic. If the Monitoring traffic is not prioritized, information is available less quickly than desired, and if it is prioritized, it may compete with other important traffic.

Nmap is a network port scanner and generated the output shown in the question: a list of network ports. Nessus is a vulnerability scanner and would produce a detailed report of vulnerabilities. Traceroute determines the path between two points on a network. Syslog is a logging facility on Linux systems.

Signature analysis uses a fingerprint or signature to detect threats or other events. This means that a signature has to exist before it can be detected, but if the signature is well designed, it can reliably detect the specific threat or event.

Wireshark is a protocol analyzer and can be used to capture network traffic in a standard format. Nessus and Nmap are vulnerability scanners. Nikto is a web application security scanner.

The Netstat tool shows all open connections on a system. Topdump and Wireshark are capable of capturing traffic from open connections but will not display connections that are silent during the capture period. Traceroute shows the path between two systems.

There are many reasons to avoid imaging live machines if it is not absolutely necessary, but one advantage that imaging a live machine has is the ability to directly capture the contents of memory. Risks of capturing images from live machines include inadvertent modification of the systems, changes that may occur on the machine during imaging, the potential for malware to attack the imaging system or to detect and avoid it, and the fact that most live images don't capture unallocated space.

Organizational change management processes are often bypassed during an incident response process due to the urgency of the need to make quick changes. Once the incident response has been completed, changes are often filed as catch - up documentation as part of the post incident activities.

The user is developing potential scenarios that might result in a successful attack. This is an example of establishing a threat - hunting hypothesis. Next, the user should look for evidence of such an attack in an attempt to confirm or refute his hypothesis,

Multi - factor authentication like token - based authentication can help prevent phishing attacks that result in stolen credentials resulting in attackers accessing systems. As long as attackers do not also acquire the token (often an app on a smartphone or a physical device kept in the user's pocket), the attacker will not have all the factors they need to authenticate. Context - aware authentication might help if attackers log in from places that legitimate users don't, but enhanced password requirements and shorter password lifespans have a relatively small impact, if any.

Unit testing tests the smallest testable parts of an application or program, ensuring that each component works properly before they are put together. UAT is user acceptance testing, Fagan inspection is a form of formal code review, and code segmentation is not a term used in software engineering or development.

Once a security incident has been detected and analyzed, CSIRTs move into an active phase of containment, eradication, and recovery. Active measures seek to limit the damage, gather evidence, identify the attackers and systems they are using, and eradicate the effects of the incident.

This is most likely a port scan being used to conduct reconnaissance and determine what ports are open on the server. A DoS attack would more likely use requests to a service allowed through the firewall. SQL injection and cross - site scripting would be successful only against a web server that was allowed to receive connections through the firewall.

Cisco uses log level O for emergency situations. Log level 1 is for alerts. Log level 6 is for information, and log level 7 is for debugging.

Since the user already knows the MAC addresses of all the devices due to her systems inventory, she can simply search for associated MAC addresses that do not match the list.

When existing controls are insufficient, do not resolve the issue, or are too difficult to implement, a compensating control is often put in place. It is important to document compensating controls, because they differ from the expected or typical control that would normally be in place.

The image shows a screenshot of network traffic captured using the Wireshark protocol analyzer.

I The -sV flag reports banner and version information. The -OG flag generates greppable output. The -sS flag requests a TCP SYN scan. The -b flag is used to detect servers supporting FTP bounce.

Encrypting a drive with strong encryption like AES 256 will make the loss of a drive less of an issue. In general, strong encryption with a key that has not also been exposed can make confidentiality risks like this negligible. Both MD5 and SHA1 are not encryption methods - they are hashes. DES is an older, weaker encryption method, and it would not provide strong protection for the drive.

It can be easy to forget how important policies and the standards and practices that derive from them are, but policies make up the foundation of an organization's security practices. When combined with awareness training, it is far more likely that the employees that Cynthia works with will avoid bad practices like taking unencrypted drives home or neglecting to use web application security development best practices.

The user's design should include an intrusion prevention system (IPS). An in - line IPS with the right signatures installed can detect and stop attacks, including SQL injection, cross - site scripting, and even denial - of - service (DoS) attacks. An intrusion detection system (IDS) could detect the attacks but can't stop them, whereas data loss prevention (DLP) systems are designed to prevent data from exiting an organization. A PRNG, or pseudo - random number generator, is not a security technology

Port 1433 is used by Microsoft SQL Server, so the user is most likely scanning a database server.

The Secure Shell (SSH) protocol uses encryption by default. HTTP, MySQL, and SMTP do not use encryption unless configured to do so.

The key difference between a shared authentication model and a single sign - on (SSO) model is that shared authentication systems require users to enter credentials when authenticating to each site. Single sign - on only requires a single sign - on - exactly as the name says!

In NIST's classification scheme, this is a privacy breach, involving personally identifiable information. NIST defines four ratings: none, privacy breaches, proprietary information breaches, and integrity loss. Proprietary information breaches involve unclassified proprietary information, such as protected critical infrastructure information Integrity losses occur when sensitive or proprietary information is changed or deleted. NIST does not use the broad term confidentiality breaches, instead preferring more specific definitions,

Port 53 is reserved for the Domain Name Service (DNS), which does not normally run on web servers. Ports 80 and 443 are used for HTTP and HTTPS, respectively. Ports in the range of 80xx are commonly used for web services running on nonstandard ports.

Perfmon (Performance Monitor) provides the ability to perform detailed data collection, unlike resmon's (Resource Monitor) high - level view, which does not include the use of counters. Winmon is a name typically associated with malware, and sysctl is a Linux tool used for changing kernel parameters at runtime.

The DNS server that answered the user's request is identified in the first line of the response. The IP addresses that appear at the bottom are the server's response to the user's query.

Chain - of - custody tracking indicates who has access to and authority over drives, devices, and forensic data throughout their life cycle. This is a critical element in investigations that may end up in court or that will involve law enforcement.

The user has created an MD5 hash of his image file. This can be compared to the original, or if it is the original, it can be compared to figure copies to validate their integrity.

Hashes are compared to verify that the files are the same.

MD5 returns a warning that the checksum did not match, we know that the files are different.

NTP (Network Time Protocol) is used to ensure that events that are logged and other actions taken that use system time line up properly. Without NTP enabled, it may be significantly more difficult to determine when events occurred, making the chronological view of events harder, or even impossible, to build.

The most important criteria when making decisions about the scope of vulnerability management programs are regulatory requirements, corporate policy, asset classification, and data classification.

PCI DSS only requires that internal scans be conducted by a qualified individual. External scans must be conducted by an approved scanning vendor (ASV).

Common Vulnerabilities and Exposures (CVE) provides a standard nomenclature for describing security - related software flaws. Common Vulnerability Scoring System (CVSS) provides a standardized approach for measuring and describing the severity of security - related software flaws. Common Platform Enumeration (CPE) provides a standard nomenclature for describing product names and versions. Open Vulnerability and Assessment Language (OVAL) is a language for specifying low - level testing procedures used by checklists.

DumpIt is a Windows - only memory forensics tool. LIME and fmem are both Linux kernel modules that allow access to physical memory, and the Volatility Framework is a multiplatform tool with support for a broad range of memory forensics activities.

The three steps in the vulnerability management life cycle are detection, remediation, and testing.

NIST uses three critical measures to determine an organization's tier in the framework: how to mature their risk management process is, whether there is an integrated risk management program, and if the organization is effectively participating with external partners.

Credentialed scanning should always be performed with a read - only account to limit the potential impact on the system should the scanner malfunction or the account become compromised.

The system should be rated as moderate impact for confidentiality if "the unauthorized disclosure of information stored on the system could have a serious impact on organizational operations, organizational assets, or individuals," according to FIPS 199.

Kerberos generating tickets, also known as golden tickets, can be created if attackers are able to gain domain administrator or local administrator access to the AD controller. This would allow attackers to set arbitrary ticket lifespans and to act as any user in the domain or forest.

LDAP attacks often focus on insecure binding methods, harvesting directory information by taking advantage of improper ACLS, LDAP injection, or denial - of - service attacks. Silver ticket attacks are associated with Kerberos, where the term is used to describe compromised service account credentials.

The most accepted commonly criteria for vulnerability prioritization include criticality of the systems and information affected by the vulnerability, difficulty of remediating the vulnerability, severity of the vulnerability, and exposure of the vulnerability.

The Federal Information Security Management Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS) both require the use of vulnerability scanning. The Gramm - Leach - Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) have no such requirement.

Testing code by running it is known as dynamic code analysis. Static code analysis looks at the source code for an application. Runtime is when a program is running, but runtime inspection is not a common term used in software engineering. There is no Run / Test method.

This describes a false positive error - the condition where a scanner reports a vulnerability but that vulnerability does not actually exist.

Technical subject matter experts, IT support staff, legal counsel, human resources staff members, and public relations and marking staff are all frequently part of the CSIRT. Comptrollers are rarely part of the response process.

IPS and firewall devices can detect scans and probes, and may have built - in detection methods. A SIEM can pull data from multiple sources, data scans and probes against a variety of devices. SNMP traps provide information about the state of a device but are not useful when attempting to detect network scans or probes.

Regression testing focuses on ensuring that changes have not reintroduced problems or created new issues. The user has asked her team to do regression testing to make sure that the patches have not created new problems or brought an old problem back.

Fault injection directly injects faults into the error handling paths of an application and focuses on areas that might otherwise be missed. Fuzzing sends unexpected data, whereas mutation testing modifies the program itself to see how it handles unexpectediors. Fagan inspection is a formal inspection process.

Windows captures quite a bit of useful data about USB devices when they are connected, but it does not capture the device's capacity. The device name, serial number, vendor, brand, and even the user ID of the currently logged - in user when it was plugged in are captured.

This process shows a Fagan inspection, which consists of six phases: Planning, Overview, Preparation, Meeting, Rework and Follow - Up.

Windows workstations can be a treasure trove of forensic information. Volume shadow copies are manual or automatic copies of files or volumes kept by Windows systems for backup.

This vulnerability is in the SSH protocol, which uses TCP port 22, as shown in the bottom portion of the graphic.

The most effective defense against SQL injection is the use of input validation Firewall rules would not likely be effective because the web server likely requires access from the outside world. Honeypots and patching would not serve as a defense against a SQL injection attack.

Buffer overflow vulnerabilities in an operating system require a vendor - supplied patch to correct. Input validation would not be an effective defense. While firewalls and intrusion prevention systems may block an attack, they would not resolve the underlying problem.

None of these protocols should be used on a secure network. All versions of SSL contain unfixable vulnerabilities, as do TLS versions earlier than 1.2.

The most effective defense against cross - site scripting is the use of input validation Firewall rules would not likely be effective because the web server likely requires access from the outside world. Honeypots and operating system patching would not serve as a defense against a SQL injection attack

Network segmentation is a strong security control for ICS networks. Chelsea does not have access to the source code so she cannot rewrite it. No patch is available because the vendor no longer provides support. Encryption would not provide a defense against a buffer overflow attack

In a virtualized datacenter, the virtual host hardware runs a special operating system known as a hypervisor that mediates access to the underlying hardware resources.

The most likely scenario is that the hotel is running a captive portal and the user must authenticate before trying to access other websites. While the other scenarios are possible, they are not as likely. If the error was with the company certificate, other users would be reporting the same problem. It is possible that another hotel guest is attempting to trick the user into accepting a false certificate, but this is unlikely.