CompTIA CySA+ (CS0-001) Practice Exam
https://www.diontraining.com

1) You have been asked to remediate a vulnerability in a server. Once you have located a patch for the vulnerability, what should happen you do NEXT?
   a) Start the incident response process
   b) Establish continuous monitoring
   c) Rescan the server to ensure the vunlnerability still exists
   d) Submit a Request for Change to begin the change management process

2) TRUE or FALSE: Organizations should always involve law enforcement if they suspect a crime was committed.
   a) TRUE
   b) FALSE

3) What is NOT a means of improving data validation and trust?
   a) Encrypting data in transit
   b) Using MD5 checksums for files
   c) Decrypting data at rest
   d) Implementing Tripwire

4) What is NOT considered part of the Internet of Things?
   a) SCADA systems
   b) ICS
   c) Internet-connected television
   d) A Windows 2016 server configured as a domain controller

5) A cyber security analyst needs to pick a tool in order to be able to identify open ports and services on a host along with the version of the application that is associated with the ports and services. They have decided to choose a command line tool, what tool did should they choose?
   a) ping
   b) nmap
   c) netstat
   d) Wireshark

6) When using nmap, what flax do you use in the syntax to conduct operating system identifcation during the scan?
   a) -os
   b) -o
   c) -id
   d) -osscan

7) A recent threat has been announced in the cyber security world stating that there is a critical vulnerability in the kernel of a particular operating system. You company, unfortunately, has not maintained a current asset inventory, so you are unsure of how many of your servers may be affected. What technique should you perform to find all affected servers within your company?
   a) Manual log review from data sent to syslog
   b) OS fingerprinting scan across all hosts
   c) Packet capture of data traversing the server network
   d) Service discovery scan on the network

8) Chris needs to ensure that accessing a drive to analyze it does not change the contents of the drive. What tools should he use?
   a) Forensic drive duplicator
   b) Hardware write blocker
   c) Software write monitor
   d) Degausser

9) TRUE or FALSE: Analysts prioritizing vulnerabilities for remediation should consider the difficulty of remediation when assigning priorities.
   a) TRUE
   b) FALSE

10) An salesperson began having issues with their laptop becoming unresponsive after attempting to open a PDF in their email. They called the cyber security analyst, who checked the IDS and antivirus software for any unusual behavior or alerts, but the analyst found nothing suspicious. What term BEST describes the this threat?
   a) Packet of death
   b) Zero-day malware
   c) PII exfiltration
   d) Known virus

11) TRUE or FALSE: Some vulnerability scans require account credentials to log on to scanned servers.
   a) TRUE
   b) FALSE

12) What method might a system administrator use to replicate the DNS information from one DNS server to another, but could also be used maliciously by an attacker?
a) Zone tranfers
b) DNS registration
c) AXR
d) DNSSEC

13) Which tool would allow you to conduct operating system fingerprinting, which typically relies on responses to TCP/IP stack fingerprinting techniques?
a) nmap
b) dd
c) scanf
d) msconfig

14) Which of the following is NOT one of the main criteria that should be included in a penetration testing plan?
a) Timing
b) Scope
c) Account credentials
d) Authorization

15) A cybersecurity analyst has received an alert that well-known “call home” messages are continuously observed by network sensors at the network boundary. The good news is that the proxy firewall was properly configured to successfully drop the messages prior to them leaving the network. These “call home” messages have been determined to be a true positive. What is MOST likely the cause?
a) Attackers are running reconnaissance on company resources
b) An infected system is running a command that is attempting to reach a botnet's command and control server
c) A malicious insider is trying to exfiltrate information to a remote network
d) Malware is running on a company workstation or server

16) What is NOT part of the security incident validation effort?
a) Scanning
b) Sanitization
c) Patching
d) Permissions

17) A cyber security analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW for an upcoming assessment of a client's network. What information is traditionally found in the SOW?
    a) Timing of the scan
    b) Contents of the executive summary report
    c) Excluded hosts
    d) Maintenance windows

18) Jamie has been tasked with finding a rogue network device on her wired network. What option is NOT likely to help identify the rogue device?
    a) MAC validation
    b) Port scanning
    c) Site surveys
    d) War-walking

19) TRUE or FALSE: Organizations may decide not to remediate vulnerabilities because of conflicting business requirements.
    a) TRUE
    b) FALSE

20) What port is most likely to be used in a web-based attack?
    a) 389
    b) 3389
    c) 443
    d) 21

21) What is the proper threat classification for a security breach that employs brute-force methods to compromise, degrade, or destroy systems?
    a) Attrition
    b) Impersonation
    c) Improper usage
    d) Loss or theft of equipment

22) Edward's IDS reports that ports 1 to 1024 received SYN packets from a remote host. What has likely happened to cause this traffic?
    a) Remote host cannot find the right service port
    b) SYN flood
    c) Port scan
    d) UDP probe

23) A company wants to remediate vulnerabilities inside its web servers. An initial vulnerability scan was performed and the cyber security analysts are now reviewing the results. The cyber security analysts want to remove false positives before starting any remediation efforts in order to avoid wasting their time on issues that are not actual vulnerabilities. What is an indicator of a something that is most likely a false positive?
   a) Reports show the scanner compliances plug-ins are not up-to-date
   b) Any items labeled 'low' are considered informational only
   c) The scan result versions are different from the automated asset inventory
   d) 'HTTPS' entries indicate the web page is encrypted securely

24) What two techniques are commonly used by port and vulnerability scanners to perform services system identification?
   a) Comparing response fingerprints and registry scanning
   b) Banner grabbing and UDP response timing
   c) Using the oslookup utility and UDP response timing
   d) Banner grabbing and comparing response fingerprints

25) The service desk has been receiving a large number of complaints from external users that a web application is responding slow to requests and frequently receives a "connection timed out" error when they attempt to submit information into the application. What software development best practice should have been implemented in order to have prevented this issue from occuring?
   a) stress testing
   b) regression testing
   c) input validation
   d) fuzzing

26) Jacob discovers a service running on one of the ports known as a registered port while running a port scanner. What does this tell him about the service?
   a) It isrunning on a well-known port (0-1023)
   b) The service's name
   c) It is running on a port between 1024 and 49151
   d) The vulnerability status of the service

27) If your DNS server allows __________ and is not properly secured, attackers may be able to get a full listing of your internal DNS information.
   a) 1-1023
   b) 1-65,534
   c) 1-512
   d) 1-128

28) If your DNS server allows ___________ and is not properly secured, attackers may be able to get a full listing of your internal DNS information.
a) Zone tranfers
b) Split horizon
c) FQDN resolution
d) Remediate the threat

29) What protocol is commonly used to collect information about CPU utilization and memory usage from network devices?
a) Netflow
b) SMTP
c) MIB
d) SNMP

30) What popular open source port scanning tool is commonly used for host discovery and service identification?
a) nmap
b) dd
c) services.msc
d) Windows Defender

31) A(n) _____________ provides organizations with an attacker's perspective on their security.
a) Vulenrability Scan
b) Asset Management
c) Penetration Test
d) Patch Management

32) Gary is interpreting a vulnerability scan report and finds a vulnerability in a system that has a CVSS access vector rating of A. What statement is correct based upon this information?
a) The attacker must have physical or logical access to the affected system.
b) Exploiting the vulnerability requires the existence of specialized conditions.
c) The attacker must have access to the local network that the system is connected to.
d) Exploiting the vulnerability does not require any specialized conditions.

33) A cryptographically weak encryption cipher
a) A cryptographically weak encryption cipher
b) A website utilizing a self-signed SSL certificate
c) A buffer overflow that is known to allow remote code execution
d) An HTTP response that reveals an internal IP address

34) What condition occurs when a scanner reports a vulnerability that does not exist?
   a) False positive error
   b) False negative error
   c) True positive error
   d) True negative error

35) Which of the folllowing is NOT a part of the vulnerability management lifecycle?
   a) Remediation
   b) Testing
   c) Detection
   d) Investigating

36) What type of scans are useful for probing firewall rules?
   a) TCP SYN
   b) TCP ACK
   c) TCP RST
   d) XMAS TREEE

37) Michelle is preparing to run an nmap scan of a targeted network. She wants to perform a quick scan but knows that a SYN scan isn't possible because she doesn't have raw socket privileges on the system she is going to conduct her scan from. What flag should she use to set her scan type?
   a) -sS
   b) -O
   c) -sT
   d) -sX

38) You have been hired as a consultant to help a company, Blueboard Enterprises, develop a new disaster recovery plan. Blueboard has recently grown in the number of employees, and so has its information systems infrastructure to support those new employees. Unfortunately, Blueboard doesn't currently have any documentation, policies, or procedures for its network. What is the first step you recommend to Blueboard's management in order to help in the development of the disaster recovery plan?
   a) Conduct a risk assessment
   b) Develop a data retention policy
   c) Execute vulnerability scanning
   d) Identify assets

39) In which tier of the NIST cybersecurity framework does an organization understand its dependencies and partners?
    a) Partial
    b) Risk informed
    c) Repeatable
    d) Adaptive

40) You have been tasked to conduct a review of the firewall logs. During your review, you notice that an IP address from within your company's server subnet had been transmitting between 125 to 375 megabytes of data to a foreign IP address during nighttime hours. Looking over the logs, you have determined this has been occuring for approximately 5 days and the affected server has since been taken offline for forensic review. What is MOST likely to increase the impact assessment of the incident?
    a) PII of company employees and customers was exfiltrated
    b) Raw financial information about the company was accessed
    c) Forensic review of the server required fall-back on a less efficient service
    d) IP addresses and other network-related configurations were exfiltrated

41) What document typically contains high-level statements of management intent?
    a) Procedure
    b) Guideline
    c) Standard
    d) Policy

42) What SDLC model emphasizes individuals and interactions over processes and tools, customer collaboration over contract negotiation, and working software over comprehensive documentation?
    a) Waterfall
    b) Spiral
    c) Agile
    d) RAD

43) A cyber security professional visited an e-commerce website by typing in its URL and found that the admininstrative web frontend for its backend e-commerce application is accessible over the Internet and is only being protected by the default password. What three things should the analyst recommend to the website owner in order to MOST securely remediate this discovered vulnerability?
   a) Rename the URL to a more obscure name, whitelist all corporate IP blocks, and require two-factor authentication
   b) Change the username and default password, whitelist specific source IP addresses, and require two-factor authentication for access
   c) Change the default password, whitelist all specific IP blocks, and require two-factor authentication
   d) Red Team all corporate IP blocks, require an alphanumeric passphrase for the default password, and require two-factor authentication

44) A penetration tester would seek to gain complete control of a system during what phase of a penetration test?
   a) Planning
   b) Attack
   c) Reporting
   d) Discovery

45) What security control provides Windows administrators with an efficient way to manage system configuration settings across a large number of devices?
   a) Patch management
   b) GPO
   c) HIPS
   d) Anti-malware

46) Nicole is investigating a security incident at a government agency and discovers that attackers obtained PII. What is the information impact of this incident?
   a) None
   b) Privacy breach
   c) Proprietary breach
   d) Integrity breach

47) You have been called into the Chief Technology Officer's (CTO) office and been asked for a recommendation concerning network monitoring services for the company's intranet. The CTO requests that your solution have the capability to monitor all traffic to and from the network's gateway and have the ability to block certain types of content. What solution should you recommend?
   a) Setup of IP fltering on the internal and external interfaces of the gateway router
   b) Installation of an IDS on the internal interface and a firewall on the external interface of the gateway router
   c) Installation of a firewall on the internal interface and a NIDS on the external interface gateway router
   d) Installation of an IPS on both the internal and external interfaces of the gateway router

48) Tony's manager requires him to receive and inventory the items that his co-worker Barbara orders. This is an example of what kind of personnel control?
   a) Separation of duties
   b) Background checks
   c) Dual control
   d) Mandatory vacation

49) William is evaluating the potential impact of a confidentiality risk and determines that the disclosure of information contained on a system could have a limited adverse effect on the organization. Using FIPS 199, how should he classify the confidentiality impact?
   a) Low
   b) Medium
   c) Moderate
   d) Higjh

50) Mary Beth is preparing her organization for the required quarterly PCI DSS external vulnerability scan. Who can perform this scan?
   a) Anyone
   b) Any qualified individual
   c) Only employees of the company
   d) Only an approved scanning vendor

51) You have been tasked to create some baseline system images in order to remediate vulnerabilities found in different operating systems. Before any of the images can be deployed, they must be scanned for malware and vulnerabilities. You must ensure the configurations meet industry standard benchmarks and that the baselining creation process can be repeated frequently. What vulnerability option would BEST create the process requirements to meet the industry standard benchmarks?
a) Utilizing an operating system SCAP plugin
b) Utilizing an authorized credntial scan
c) Utilizing a non-credential scan
d) Utilizing a known malware plugin

52) If there is an expected loss of ______ or more, then the federal government classifies the economic impact of a security incident as high.
a) $1
b) $10,000
c) $100,000
d) $500,000

53) Liberty Beverages allows its visiting business partners from SodaCorp to use an available Ethernet port in the Liberty Beverage conference rooms when they are in the building. This access is provided to allow employees of SodaCorp to have the ability to establish a VPN connection back to the SodaCorp network. You have been tasked to ensure that SodaCorp employees can gain direct Internet access from the Ethernet port in the conference room only. But, if a Liberty Beverage employee uses the same Ethernet port, they should be able to access Liberty's internal network, as well. What should you use to ensure this capability?
a) ACL
b) SIEM
c) MAC
d) NAC

54) What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assests scanned accurately?
a) Processor utilization
b) Virtual hosts
c) Organizational governance
d) Log disposition

55) Johnny wants to make sure he receives logs for his Cisco devices that indicate when they shut down due to failure. What level of log level message should should Johnny configure his devices in order to receive these types of messages?

a) 0
b) 2
c) 5
d) 7

56) Your organization needs to institute an organizational vulnerability management program due to new regulations. The CIO assigns this new function to the information security team. What framework would BEST support the program?

a) NIST
b) OWASP
c) SDLC
d) SANS

57) What is NOT on of the factors that comprise the exploitability score for a vulnerability?

a) Access vector
b) Authentication
c) Access complexity
d) Availability

58) What regulation protects the privacy of student educational records?

a) HIPPA
b) FERPA
c) SOX
d) GLBA

59) You received an incident response report that indicates a piece of malware was introduced into the company’s network through a remote workstation that was connected to the company’s servers over a VPN connection. You have been askd for a recommendation to solve this issue: what control should be applied to prevent this type of incident from occuring in the future?

a) ACL
b) NAC
c) TAP
d) MAC filtering

60) What vulnerability invovles leveraging access from a singel virtual machine to other machines on the network?
   a) VM escape
   b) VM migration
   c) VM reuse
   d) VM vulnerability

61) What describes the infrastructure needed to support the other architectural domains in the TOGAF framework?
   a) Business architecture
   b) Applications architecture
   c) Data architecture
   d) Technical architecture

62) You should provide training to all your employees about the proper incident communication channels to use during a security event
   a) You should ask all employees to commit to an NDA about the data breach verbally
   b) You should ask all employees to commit to an NDA about the data breach verbally
   c) You should block all employee access to social media from the company's network
   d) You should ask a member of law enforcement to meet with your employees

63) Based on some old SIEM alerts, you have been asked to perform some forensic analysis on a particular host. You ahve noticed that some SSL network connections are occurring over ports other than port 443. Additionally, the SIEM alerts state that copies of svchost.exe and cmd.exe have been found in the %TEMP% folder on the host, as well as showing that RDP connections have previously connected with an IP address that is external to the corporate intranet. What threat might you have uncovered during your analysis?
   a) DDoS
   b) APT
   c) Ransomware
   d) Software vulnerability

64) Betsy has been asked to perform an architectural review and uses a view that focuses on the technologies, settings, and configurations used in the architecture. What view is she using?
   a) Operational view
   b) Acquisition view
   c) Technical view
   d) Logical view

65) A cyber security technician has been running an intensive vulnerability scan to detect which ports might be open to exploitation. But, during the scan, one of the network services became disabled and this impacted the production server. What information source could be used to evaluate which network service was interrupted?
  a) Syslog
  b) Network mapping
  c) Firewall logs
  d) NIDS

66) What is the term for the company's willingness to tolerate risk in their computing environment?
  a) risk appetite
  b) risk acceptance
  c) risk mitigation
  d) risk avoidance

67) Your organization's primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. The critical patch designed to remediate a vulnerability that can allow a malicious actor to remotely execute code on the server from over the Internet. However, you just ran a vulnerability assessment scan of the network and found that all of the servers are still being reported as having the vulnerability. Why is the scan report still showing a vulnerability even though the patch was installed by the system adminstrators?
  a) Your vulnerability assessment scan is returning false positives
  b) The critical patch did not remediate the vulnerability
  c) You did not wait enough time after applying the patch before running the vulnerability assessment scan
  d) You scanned the wrong IP range during your vulnerability assessment

68) What provides the detailed, tactical information that CSIRT members need when responding to an incident?
  a) Procedures
  b) Guidelines
  c) Policies
  d) Instructions

69) Which party in a federation provides services to members of the federation?
   a) IdP
   b) AP
   c) RP
   d) IP

70) What secure coding practice helps to ensure characters like <, >, /, and ‘ are not accepted from the data provided by users?
   a) Risk assessment
   b) User output validation
   c) Error message management
   d) User input validation

71) What tool is NOT useful for capturing Windows memory data for forensic analysis?
   a) Fmem
   b) Volatility Framework
   c) DumpIt
   d) EnCase

72) You are a cyber security analyst sitting in an working group that is updating the incident response communications plan. A coworker, a business analyst, suggests that if the company suffers from a data breach that the correct action would to to only notify the affected parties in order to minimize the chances of the company receiving bad publicity from the media. What should you recommend to the working group in response to the buisness analyst’s recommendation?
   a) The first responder should contact law enforcement upon confirmation of a security incident in order for a forensic team to preserve the chain of custody
   b) Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance
   c) An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised resource
   d) The Human Resources department should have information security personnel who are invovled in the investigatio n of the incident sign non-disclosure agreeemtns so the company cannot be held liable for customer data that might be viewed during an investigation

73) What remediation strategies is MOST effective in reducing the risk to an embedded ICS from a network-based compromise?
    a) Patching
    b) NIDS
    c) Firewalling
    d) Disabling unused services

74) Joe and Mary work together to review Joe's code with Mary explaining the code he wrote as he reviews it. What code review technique are Joe and Mary using?
    a) Pair programming
    b) Dual control
    c) Over-the-shoulder
    d) Tool assisted review

75) What is NOT a vulnerability scanning tool?
    a) Nessus
    b) QualysGuard
    c) NExpose
    d) Zap

76) What does the bs operator do when using the Linux dd command?
    a) Sends output to a blank sector
    b) Sets the beginning sector
    c) Sets the block size
    d) Removes error messages and other incorrect data

77) A cyber security analyst has been hired to perform an assessment of a company's current security posture. The analyst first would like to determine how much information about the company is exposed to an external attacker. What technique would BEST help the analyst?
    a) DNS query log reviews
    b) Intranet portal reviews
    c) Fingerprinting
    d) Technical control audits

78) What is an insecure protocol that should not be used?
    a) Telnet
    b) SSH
    c) SFTP
    d) HTTPS

Answers To CySA+ Practice Exam:

1) **D**- - Before any changes to a baseline occurs, a Request for Change for be submitted which in turn starts the change management process. Once approved, the patch should be installed on the server, then the server should be rescanned to ensure the vulnerability no longer exists.

2) **B**- The organization should consult with management and legal counsel to decide whether to involve law enforcement.

3) **C**- While encrypting data, hashing files using MD5 to check against known valid checksums, and implementing a file integrity monitor are all methods of improving data validation and trust, decrypting data at rest does not improve your ability to trust it!

4) **D**- Supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS) are examples of IoT implementations.

5) **B**- Nmap sends specially crafted packets to the target host(s) and then analyzes the responses to determine the open ports and services running on those hosts. In addition, nmap can determine the versions of the applications being used on those ports and services. Nmap is a command line tool for use on Linux, Windows, and OS X systems.

6) **B**- The -o flag tells nmap to identify the operating systems during the scanning process by evaluating the responses it received during the scan to its database/signatures for each operating system.

7) **B**- By utilizing operating system fingerprinting using a tool like nmap, you can identify which servers are running which version of the operating system. This will give you an accurate list of the possibily affected servers.

8) **B**- Hardware and software write blockers are designed to ensure that forensic software and tools cannot change a drive inadvertently by accessing it. Forensic drive duplicators copy drives and validate that they match the original, software write monitors are not used for forensic use like this, and a degausser is used to wipe magnetic media.

9) **A**- Difficulty of remediation is one of the criteria that analysis should consider. They should also consider the criticality of the system and information, severity of the vulnerability, and exposure of the vulnerability.

10) **B**-This threat is a zero-day malware. Since it is a new piece of malware, a signature has not been created for the antivirus or IDS defintions file. This type of malware cannot be combatted with traditional signature-based methods, such as anti-virus or an IDS.

11) **A**- Credentialed scans use read-only accounts to log on to the servers being scanned and retrieve configuration information.

12) **D**-Zone transfers provide an easy way to send all the DNS information from one DNS server to another, but it could also be used by an attacker for reconnaissance against your organization. For this reason, most administrators disable zone transfers from untrusted servers. (AXR was a made up term to confuse you with AXFR, which is the command used to conduct a zone transfer.)

13) **A-** OS identification relies on differences in how operating systems and even operating system versions respond, what TCP options they support, what order they sent packets in, and other details that, when combined, can provide a reasonably unique fingerprint for a TCP stack.

14) **C**- The three main criteria that should be included in a penetration testing plan are timing, scope, and authorization.

15) **B**- The “call home” message is indicative of beaconing. This usually occurs after a stage 1 malware has been implanted on a company’s workstation or server, but the more correct answer is that this infected system is running a command that is attempting to reach a botnet’s command and control server. This beaconing will continue until the infected host (workstation or server) is found and cleared of the malware, or until the botnet gives the infected host further instructions (such as to attack).

16) **B**- Patching, permissions, scanning, and verifying logging are the components of the security incident validation effort. Sanitization is a component of the security incident eradication effort.

17) **C**- It is routine and normal that the Scope of Work (SOW) contains the list of excluded hosts. This ensures that the penetration tester does not affect hosts, workstations, or servers outside of their scope of the assessment.

18) **D**- While checking valid MAC addresses against a known list, scanning for new systems or device, and physically surveying for unexpected systems can be helpful, war-walking (surveying for wireless networks and devices) won’t help find a wired rogue device.

19) **A**- Organizations may make risk-based decisions not to remediate vulnerabilities. In those cases, they should create a documented exception.

20) **C**- Port 389 is used by LDAP, Port 21 is used by FTP, and port 3389 is used by RDP. Web-based attacks would likely appear on port 80 (HTTP) or port 443 (HTTPS)

21) **A**- Attrition attacks employ brute-force methods to compromise, degrade, or destroy systems, networks or services.

22) **C**- A SYN scan may connect to each possible open port on a remote system, triggering an IDS. While scanners support more stealthy scans, default scans may connect to each port in turn. Remote hosts will typically connect to only a single port associated with a service, a SYN flood normally sends many SYNs to a single system but doesn’t send them to unused ports, and a UDP probe will not send SYN packets.

23) **B**- When conducting a vulnerability assessment using a vulnerability scanner, it is common for the scanner to report some things are “low” priority or “for informational purposes only”. These are most likely false positives and can be ignored by the analyst when starting their remediation efforts.

24) **D**- Service and version identification is often performed by grabbing service banners and checking responses for services to known fingerprints of those services. UDP response timing, along with other TCP/IP stack fingerprinting techniques, are used to identify operating systems, while oslookup is not an actual utility.

25) **A**- Stress testing is a software testing activity that determines the robustness of software by testing beyond the limits of normal operation. Stress testing is particularly important for "mission critical" software, but is used for all types of software. This stress testing is an important component in the capacity management process of IT service management and is used to ensure adequate resources are available to support the needs of the end user once the service or application goes into the production environment.

26) **C**- John knows that the ports known as “registered ports” between 1024 and 49151 are assigned by the Internet Assigned Numbers Authority but that using one of those ports is not a guarantee that the service matches what is typically run on it. Discovering a service using a port scanner doesn’t necessarily identify the service correctly, and ports between 0 and 1023 are known as the “well-known” or “system” ports.

27) **A**- The well-known ports are numbered from 1-1023. Ports above this number are called ephemeral ports. While these ports are commonly associated with specific services, they can be used for any service. Users or applications just need to be made aware of what port to access the service on.

28) **A**- DNS zone transfers provide a full listing of DNS information. Improperly secured DNS servers may allow attackers to gather this data by performing a zone transfer.

29) **D**- Simple Network Management Protocol (SNMP) is commonly used to gather information from routers, switches, and other network devices. It provides information about a device's status including CPU and memory utilization as well as many other useful details about the device. Netflow provides information about network traffic, MIB is a management information block, and SMTP is the Simple Mail Transfer Protocol.

30) **A**- Nmap is a popular open source port scanning utility.

31) **C**- Penetration tests provide organizations with an attacker's perspective on their security. The NIST process for penetration testing divides tests into four phases: planning, discovery, attack, and reporting. The results of penetration tests are valuable security planning tools, as they describe the actual vulnerabilities that an attacker might exploit to gain access to a network.

32) **C**- The access vector explains what type of access that the attacker must have to a system or network and does not refer to the types of specialized conditions that must exist. In this case, the A rating refers to Adjacent Network, and the attacker must have access to the local network to exploit the vulnerability.

33) **C**- The most serious vulnerability discovered is one that could allow remote code execution to occur. Since this buffer overflow is known to allow remote code execution, it must be mitigated first to most effectively prevent a security breach.

34) **A**- False positive errors occur when a scanner reports a vulnerability that does not actually exist on a system.

35) **D**- The three phases of the vulnerability management lifecycle are detection, remediation, and testing.

36) **B**- TCP ACK scans can help to determine what services are allowed through a firewall.

37) **C**- Nmap’s TCP scan function is enabled using the -sT flag and is a quick way to scan when you are unable to get raw socket access to the scanner system. Fast scans are more frequently conducted using the -sS (SYN) scan, but it requires raw socket access.

38) **D**- The first step to developing an effective disaster recovery plan is to understand exactly what assets your organization has. This requires the identification of assets. Once identified, you can then determine what assets and services are essential to business operations and how best to recovery in the event of a disaster.

39) **C**- In the repeatable tier (Tier 3) of the NIST CSF, the organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

40) **A**- If the PII (Personally Identifiable Information) of the company’s employees or customers was exfiltrated or stolen during the compromise, this would increase the impact assessment of the incident. Loss of PII is a large issue for corporations and one that might garner media attention, as well.

41) **D**- Policies are high-level statements of management intent. Compliance with policies is mandatory. An information security policy will generally contain broad statements around cybersecurity objectives.

42) **C**- The Agile Manifesto, the underlying document behind the Agile SDLC model, emphasizes individuals and interactions over the processes and tools that Spiral and Waterfall rely on. It also calls out working software, customer collaboration, and responding to change as key elements of the Agile process.

43) **B**- Since the application was only protected by the default password, the username and password should be changed immediately to increase the security of the application. Since this is an administrative frontend, only a few machines should require access and they should specifically have their IP addresses added to the whitelist and deny all other machines from accessing the administrative frontend. Finally, since this is an administrative frontend, it is a best practice to utilize two-factor authentication in order to most effectively secure the application from attack.

44) B- During the attack phase, the attacker seeks to gain access to a system, escalate that access to obtain complete control, and then conduct browsing to identify mechanisms to gain access to additional systems.

45) **B**- Patch management, host intrusion prevention systems (HIPS), and antimalware software all good host security controls, but only Group Policy Objects (GPOs) provide the ability to configure settings across multiple Windows devices.

46) **C-** In a privacy breach, sensitive personally identifiable information (PII) was accessed or exfiltrated.

47) **C**- n order to meet the requirement to monitor all traffic to and from the network's gateway, it is best to utilize a network intrusion detection system (NIDS) that monitors the external interface of the gateway router. In order to be able to block certain types of content, it is best to install a firewall on the internal interface, where ACLs can be established for those traffic types.

48) **A**- Tony's manager is using separation of duties to ensure that neither Barbara nor Tony can exploit the organization's ordering processes. Dual control, the most likely other answer, requires two employees to perform an action together.

49) A- FIPS 199 classifies any risk where "the unauthorized disclosure of information could be expected to have a limited adverse effect" as a low impact confidentiality risk.

50) **D**- Quarterly required external vulnerability scans must be run by a PCI DSS approved scanning vendor (ASV).

51) **A**- The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization.

52) **D**- The federal government uses the threshold of $500,000 to distinguish high-impact breaches. Medium-impact breaches are between $10,000 and $500,000. Low-impact breaches are between $1 and $10,000.

53) **D**- NAC should be used, so that the laptop being connected can be scanned and determine if it meets the normal baseline for a Liberty Beverage laptop. If it does, it can be given access to the company's internal network. If not, it can be placed in a different subnet and given access only to the Internet.

54) **B**- Vulnerability reports should include not just physical hosts but also virtual hosts. A common mistake of new cyber security analysts is to only include physical hosts, thereby missing a large number of assets on the network.

55) **A**- Cisco log levels range from 0 for emergencies to 7 for debugging.

56) **A**- NIST (National Institute of Standards and Technology) produced a useful patch and vulnerability management program framework in its Special Publication (NIST SP 800-40).

57) **D**- The three components that make up the exploitability score are the access vector, authentication, and access complexity.

58) **B**- The Family Educational Rights and Privacy Act (FERPA) requires that educational institutions implement security and privacy controls for student educational records.

59) **B**- Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement. When a remote workstation connects to the network, NAC will place it into a separate portion of the network (sandbox), scan it for malware and its security controls, and based on the results of those scans either connect it to the company's networks or place the workstation into a separate quaranteed network.

60) **A**- Virtual machine escape vulnerabilities are the most serious issue that may exist in a virtualized environment. In this attack, the attacker has access to a single virtual host and then leverages that access to intrude on the resources assigned to a different virtual machine.

61) **D**- TOGAF divides architecture into four domains. Business architecture defines governance and organization and explains the interaction between enterprise architecture and business strategy. Applications architecture includes the applications and systems an organization deploys, the interactions between those systems, and their relation to business processes. Data architecture provides the organization's approach to storing and managing information assets. Technical architecture describes the infrastructure needed to support the other architectural domains.

62) **D**- Since the data breach is the subject of an active law enforcement investigation, you should request that a representative of the law enforcement agency speak with your employees to give them clear guidance on what they can and cannot say to people outside of the investigation.

63) **B**- The provided indicators of compromise appear to be from an Advanced Persistent Threat (APT). These attacks tend to go undetected for several weeks or months, and utilize secure communication to external IPs as well as Remote Desktop Protocol connections to provide the attackers with access to the infected host.

64) **C**- Technical views focus on technologies, settings, and configurations. Operational views look at how a function is performed or what it accomplishes, while a logical view describes how systems interconnect. Acquisition views focus on the procurement process.

65) **A-** The syslog server is a centralized log management solution. By looking through the logs on the syslog server, the technician could determine which service failed on which server, since all the logs are retained on the syslog server from all of the network devices and servers.

66) **A**- An organization's willingness to tolerate risk in their computing environment is known as the organization's risk appetite.

67) **B**- If the patch was installed properly (which the question states it was), then the only reasonable answer is that the critical patch was coded incorrectly and does not actually remediate the vulnerability. While most operating system vendors do test their patches prior to release, with extremely critical patches, sometimes they are rushed into release to the customers and the patch doesn't actually remediate the vulnerability and a second patch will be required.

68) **A**- Procedures provide detailed, tactical information to the CSIRT. They represent the collective wisdom of team members and subject-matter experts.

69) **C**- Relying parties (RPs), provide services to members of a federation. An IdP, or identity provider, provides identities, makes assertions about those identities, and releases information about the identity holders. AP and IP are both not types of parties in a federation.

70) **D**- User input validation is a critical control in secure coding efforts. It seeks to remove dangerous inputs and to make sure that applications only receive the inputs that they expect and can handle.

71) **A**- The Volatility framework, DumpIt, and EnCase all provide Windows memory capture for forensic use. Fmem and LiME are both Linux-only kernel modules that provide access to physical memory.

72) **A**- Anytime a data breach occurs, your company should first contact local, state, or federal law enforcement so that their forensically qualified investigators can collect the appropriate evidence and maintain the chain of custody.

73) **D**- By disabling unused services, the footprint of the embedded ICS is reduced and this most effectively reduces its risk to a network-based attack or compromise.

74) **C-** Over-the-shoulder code reviews rely on a programmer explaining their code to a peer, providing a chance for review and better understanding for both coders. Pair programming alternates between programmers, with one strategizing and reviewing it while the other writes code. Dual control is a personnel security process, and tool-assisted reviews are conducted using a software tool.

75) **D**- Zap is an application proxy. Nessus, QualysGuard, and Nexpose are all vulnerability scanners.

76) **C**- The bs operator sets the block size when using the Linux dd command.

77) **C**- Footprinting is the blueprinting of the security profile of an organization, undertaken in a methodological manner. Footprinting is one of the three pre-attack phases. If fingerprinting is conducted from outside of the company's network, it can be used to determine the network devices and information available to an unauthorized and external attacker.

78) **A**- Telnet uses cleartext transmission of authentication credentials and should be replaced with the secure shell (SSH) protocol.