This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

1. Heidi is on the verge of concluding an incident investigation. As she closes out her investigation, she is trying to decide what to do with all of the evidence she collected. What should be her optimal course of action?
    a) Review her organization's retention policy and comply with those instructions
    b) Securely destroy the files now and document the event
    c) Wait for instructions from law enforcement,
    d) Preserve the files indefinitely, so the evidence is preserved.
2. Michael is presently engaged in reviewing and updating the firewall rules implemented by his organization to effectively respond to evolving needs. What primary type of control does the network firewall predominantly represent?
    a) Detective
    b) Deterrent
    c) Corrective
    d) Preventive
3. Frank is Deploying A Zero-Trust Network Architecture for his organization. When following this approach, which one of the following characteristics would be important in validating a login attempt (Choose 3) ?
    a) Identity Verification
    b) IP address
    c) Geolocation
    d) Device Authentication
    e) MAC address
4. How do honeytokens differ from honeypots?
    a) Honeytokens are used for offensive cybersecurity, while honeypots are defensive.
    b) Honeytokens are physical devices, while honeypots are virtual.
    c) Honeytokens are false pieces of information, while honeypots are entire simulated systems.
    d) Honeytokens are only used by government agencies, while honeypots are used by private companies.
5. Gay is asking Carolyn about an access control vestibule that has two sets of interlocking doors inside a small space where the first set of doors must close before the second set opens. What is this type of access controlled called?
    a) Tailgating
    b) Mantrap
    c) Security Guards
    d) Multifactor
    e) Solution
6. What is a backout plan?

a) A strategy for recovering from a data breach.
b) A plan for reversing changes made during a system upgrade or implementation.
c) A method for encrypting sensitive data during transmission.
d) A protocol for preventing unauthorized access to network resources.

7. Jeremy's company operates its web server to facilitate consumer purchases through its platform. Recently, Jeremy who is a Cybersecurity engineer has received complaints regarding users encountering difficulties accessing the secure section of the website. Upon investigation, the general site appears to be functioning correctly, but the specific area designated for transactions remains inaccessible. What could be the primary cause of this issue?
   a) The firewall is blocking TCP port 80.
   b) The firewall is blocking TCP port 443.
   c) The security module of the web server is malfunctioning.
   d) The web server is down.
8. Teri is proposing the adoption of Git for all developers in her organization due to an upcoming change management process that will impact the organization's security posture. What facet of cybersecurity is Teri addressing with this recommendation?
   a) Compiler
   b) Vulnerability Testing
   c) Load Testing
   d) Version Control
9. Sarah, a Cybersecurity engineer, is designing and implementing an integrated system encompassing hardware, software, policies and procedures to oversee the entire spectrum of digital certificates. What is this comprehensive system referred to as?
   a) Internet Protocol Security (IPSec)
   b) Secure Sockets Layer (SSL)
   c) Group Policy Object (GPO)
   d) Public key infrastructure (PKI)
10. June is gathering information and requirements on multiple hardware platforms to ensure strong encryption. She has decided to make it mandatory that the server support a hardware-based security chip, that provides a secure boot process and system integrity, and secure key storage and generation. What cryptographic tools is she asking for? (Choose 3)
    a) TPM
    b) HSM
    c) KMS
    d) PKI
    e) LDAPS
    f) OCSP

11. What is the purpose of a blockchain?
    a) To store large amounts of data
    b) To decentralize information and transactions
    c) To encrypt sensitive information
    d) To create virtual reality environments
12. Which cryptographic algorithm is commonly used for generating digital signatures in X.509 certificates?
    a) RSA
    b) DES
    c) SHA-256
    d) AES
13. For years, Dean's enterprise has been careless with customer information, teetering on the edge of recklessness. Though no major breaches have occurred to endanger the organization or its clientele, a prevailing belief within the company is that a significant leak is inevitable. Dean is determined to ensure that the enterprise faces accountability for its handling of customer data so he exploits the data vulnerability to force the company to adopt stricter protocols to protect customers' information. Based on his behavior, which of the following best describes Dean?
    a) Hacktivist
    b) Insider
    c) State actor
    d) Script kiddy
14. Which risk management approach involves actively seeking to minimize risk?
    a) Transference
    b) Assessment
    c) Mitigation
    d) Avoidance
15. Which of the following best defines the term "threat actor" in the context of cybersecurity?
    a) A person or entity that develops security protocols
    b) An individual or group that exploits vulnerabilities for malicious purposes
    c) A government agency responsible for cyber defense
    d) A software tool designed to detect security breaches
16. What distinguishes a "motivation" from a "threat actor" in cybersecurity?
    a) Motivation refers to the intent behind a cyberattack, while threat actor refers to the individuals carrying out the attack
    b) Motivation refers to the type of malware used, while threat actor refers to the targeted system

c) Motivation refers to the geographic location of the attack, while threat actor refers to the time of occurrence
d) Motivation refers to the frequency of cyberattacks, while threat actor refers to the severity of the impact

17. What is the primary goal of a threat actor who is motivated by financial gain?
    a) To access sensitive information for personal use
    b) To disrupt critical infrastructure systems
    c) To steal money or valuable data
    d) To gain political leverage
18. Which threat actor motivation often involves the theft of intellectual property or trade secrets?
    a) Financial gain
    b) Espionage
    c) Environmental activism
    d) Ideological beliefs
19. A threat actor motivated by ideological beliefs is most likely to engage in which type of cyber activity?
    a) a) Conducting cyber espionage for financial gain
    b) b) Disrupting systems to further a political agenda
    c) c) Selling stolen data on the black market
    d) d) Exploiting vulnerabilities to gain unauthorized access
20. What distinguishes a state-sponsored threat actor from other types of threat actors?
    a) They are motivated solely by financial gain
    b) They operate independently without any affiliations
    c) They receive support and resources from a government entity
    d) They target only specific industries for cyber attacks
21. Eric, a user on the company network, attempts to access a website from his desktop. When he enters the URL https://www.Mysite.com, his browser displays a certificate mismatch warning. Surprisingly, there's no warning when he tries to access http://https://getcertified4less.com/. What kind of attack does this scenario represent?
    a) A. On-path
    b) B. Domain hijacking
    c) **C**. DNS poisoning
    d) D. Evil twin
22. Teri, a cybersecurity engineer is on work travel and finds herself in need of a charging station at the airport but is concerned about the security of her data. To safeguard against potential data breaches, she opts to employ one of the following tools to prevent hackers from accessing her sensitive information?
    a) A. USB data blocker

b) B. Faraday cage
c) C. Proximity reader
d) D. Cable lock

23. A Chief Security Officer seeks a solution that enhances scalability and flexibility for the back-end infrastructure, enabling seamless updates and modifications without service disruptions. The security architect emphasizes the importance of reducing back-end server resources and clarifies that session persistence is not crucial for the applications running on these servers. Which option below would MOST effectively fulfill these criteria?
    a) Reverse proxy
    b) DLP
    c) Snapshots
    d) NIC teaming
    e) VPN
24. Ryan seeks a cost-effective solution to centralize security log aggregation across his organization. Among the options listed, which tool would most effectively fulfill his requirements?
    a) Journalctl
    b) Syslog
    c) NXlog
    d) Wireshark
25. Your manager is looking to harden the network environment by ensuring clients are receiving IP addresses only from authorized DHCP servers and wants to prevent malicious ARP traffic on the network. What switch features should you enable to accomplish this result? (Choose two)
    a) MAC filtering
    b) DHCP Snooping
    c) VLAN provisional
    d) ARP inspection
    e) DNS inspections
26. Which of the following operating environments is most likely to contain a SCADA system? (Choose 3)
    a) Energy
    b) Manufacturing
    c) Consulting
    d) Logistics
    e) Retail
    f) Education

27. Gwendolyn a network administrator configures an email server to use secure protocols. When the upgrade is completed, which of the following ports on the firewall should be configured to allow for connectivity? (Choose three.)
    a) TCP 25
    b) TCP 110
    c) TCP 143
    d) TCP 389
    e) TCP 587
    f) TCP 993
    g) TCP 995 also 465, SMTPS
28. Which of the following describes a social engineering technique that seeks to exploit a person's sense of urgency?
    a) A phishing email stating a cash settlement has been awarded but will expire soon
    b) A smishing message stating a package is scheduled for pickup
    c) A vishing call that requests a donation be made to a local charity
    d) A SPIM notification claiming to be undercover law enforcement investigating a cybercrime
29. Michael, a help desk team lead, contacts Carolyn the systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When Carolyn tries to use a remote desktop to log in to the server, she sees the GUI crashed. Which of the following methods or tools can Carolyn use to troubleshoot the server effectively and securely?
    a) SFTP
    b) SSH
    c) VNC
    d) MSRA
30. Nina is examining application logs to identify the origin of a breach and discovers the following log entry: https://www.GC4LESS.com/login.php?id='%20or%20'1'1='1. What type of attack has Nina found?
    a) DLL Injection
    b) API attack
    c) SQLi
    d) XSS
    e) DoS
    f) MitM
    g) BEC
31. An audit has uncovered the presence of personally identifiable information (PII) being used in the development environment of a crucial application. Danielle, the Chief Privacy Officer (CPO), is insistent that this data be eliminated. However, the

development team expresses concerns that without actual data, they cannot effectively conduct functionality tests or search for specific information. What approach should Carolyn a security professional take to most effectively address the needs of both the CPO and the development team?

a) Data anonymization
b) Data encryption
c) Data masking
d) Data tokenization

32. Teri's organization recently fell victim to a zero-day attack. Which of the following security controls is most likely to have alerted Teri that suspicious activity was underway, despite the attack exploiting a previously unknown vulnerability?
    a) Application control
    b) Signature-based antivirus
    c) Vulnerability scans
    d) Intrusion prevention systems
33. Bryan a forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:
    <aref=https://www.mycompany.com/fundtransfer?=00001111&acct=22223334&amount=250 >Click here to unsubscribe
    Which of the following will Bryan MOST likely determine has occurred?
    a) SQL injection
    b) Broken authentication
    c) XSS
    d) XSRF
34. What is the primary risk associated with sideloading applications?
    a) Exposure to malware and unauthorized access.
    b) Incompatibility with the device's operating system.
    c) Slower performance due to untested code.
    d) Accidental deletion of important system files.
35. Carolyn is the head of cybersecurity for a major corporation and she just received alarming reports of a breach in the network. Her team rushes to investigate, uncovering a sophisticated attack. As Carolyn analyzes the situation, she realizes that multiple forms of malware are at play, each contributing to the chaos. Her CIO, Nina asks, "Which form of malware is most likely to collaborate with other types?" What does Carolyn tell Nina?
    a) A. Trojan horse
    b) B. Ransomware

c) C. Rootkit
d) D. Spyware

36. Karla is logging in to her bank account on a public Wi-Fi network. Cody, an attacker, eavesdrops on the communication between Karla's computer and the bank's server. He captures the data packets containing Karla's login credentials. Which of the following scenarios could result from a replay attack by Cody?
    a) The attacker can decrypt Karla's login credentials and steal her money directly.
    b) The attacker can trick the bank's server into thinking Cody is Karla and log in to her account.
    c) The attacker can inject malware onto Karla's computer to steal her information later.
    d) The attacker can disable Karla's online banking access.
37. Which of the following security measures would be MOST effective in preventing a replay attack on a login system?
    a) Using a strong password
    b) Implementing two-factor authentication (2FA)
    c) Encrypting data in transit with HTTPS
    d) Using a virtual private network (VPN) on public Wi-Fi
38. In a complex software system, engineers are deliberating on how to enhance its robustness. They understand the importance of ensuring that the failure of one process doesn't adversely affect another. Which design principle should they prioritize to achieve this goal?
    a) Information/Data Hiding
    b) Resource Encapsulation
    c) Process Isolation
    d) Simplicity of Design
39. Joe, a hacker, breaks into a company and finds a computer that contains a file he is trying to retrieve. The file appears to be garbled, a nonsensical jumble of letters and numbers. What technology could have been used to scramble this file, it can only be read by a user who has a key or a password.
    a) Data encryption.
    b) Data transmission.
    c) Data protection.
    d) Data masking.
40. Mark, a systems administrator is setting up server services and he wants to have a terminal server with the utmost security. Which two methods should Mark use to secure the server?
    a) Change the default access port
    b) Enforce password complexity
    c) Put the terminal server into the router's DMZ

d) Disable logon time restrictions
e) Block all unused ports on the LAN
f) Use the local CAs for server authentication

41. Which of the following best defines Risk Transference in the context of cybersecurity?
    a) Outsourcing all security responsibilities to a third-party vendor
    b) Accepting the risk associated with a security threat
    c) Shifting the financial consequences of a security incident to an insurance provider
    d) Implementing multiple layers of defense to mitigate risks
42. Teri is a cybersecurity analyst working for a large company that recently implemented SDN to improve network flexibility and management. One morning, she received an alert indicating unusual activity on the network. Teri discovers that a hacker has access that allows them to manipulate the network traffic flow, potentially leading to a data breach or even a complete network shutdown. Which key components of the SDN have been infected?
    a) Control plane and data plane
    b) Hardware and software layers
    c) Physical and virtual networks
    d) Inbound and outbound traffic
43. What is a potential benefit of using IaC?
    a) Increased infrastructure complexity
    b) Decreased scalability
    c) Enhanced consistency and repeatability
    d) Longer deployment times.
44. When comparing the security implications of monolithic architecture and microservices architecture, which statement is true?
    a) Microservices architecture typically leads to simpler security management.
    b) Monolithic architecture provides better fault isolation between components.
    c) Microservices architecture often results in increased attack surface area.
    d) Monolithic architecture is more easily scalable than microservices architecture.
45. Which of the following is a characteristic of a serverless architecture from a security perspective?
    a) Greater control over underlying infrastructure
    b) Reduced attack surface compared to traditional server-based models
    c) Longer response times to security incidents
    d) Higher operational overhead for security management
46. What security challenge is commonly associated with distributed architecture?
    a) Difficulty in enforcing centralized security policies
    b) Limited scalability

c) Reduced complexity of security configurations
d) Lower risk of data breaches

47. Vincent is interested in deploying a cutting-edge security platform capable of seamlessly coordinating access policies across the diverse array of cloud providers utilized by his organization. Which technology would be most suitable for fulfilling his requirements?
    a) CASB
    b) SIEM
    c) NGEP
    d) NGFW
48. What does EAP stand for in the context of cybersecurity?
    a) Extended Authorization Protocol
    b) Endpoint Authentication Protocol
    c) Extensible Authentication Protocol
    d) Enhanced Access Protection
49. Which of the following cybersecurity solutions is designed to protect web applications from various attacks such as SQL injection and cross-site scripting?
    a) EAP
    b) WAF
    c) UTM
    d) NGFW
50. A Unified Threat Management (UTM) device typically combines which of the following security features into a single platform?
    a) Firewall, antivirus, and intrusion prevention
    b) VPN, endpoint protection, and encryption
    c) Data loss prevention, sandboxing, and vulnerability scanning
    d) Load balancing, content filtering, and SSL inspection
51. 4. What does NGFW stand for in the context of cybersecurity?
    a) Next-Generation Firewall
    b) New Generation Web Filtering
    c) Network Gateway Firewall
    d) National Grid Firewall
52. Which type of server acts as an intermediary between clients and other servers, serving as a gateway for requests from clients seeking resources from those servers?
    a) Jump Server
    b) Proxy Server
    c) Load Balancer
    d) File Server
53. Which cybersecurity solution is specifically designed to prevent unauthorized access to a network by monitoring and blocking potentially malicious activities?

a) IPS
b) IDS
c) WAF
d) VPN

54. Which of the following acronyms refers to a security architecture that combines wide-area networking capabilities with comprehensive security functionalities, often delivered as a cloud service?
    a) SASE
    b) SD-WAN
    c) WAF
    d) UTM
55. What does SD-WAN stand for in the context of networking and cybersecurity?
    a) a) Secure Data Wide-Area Network
    b) b) Software-Defined Wide-Area Network
    c) c) Secure Domain Web Access Network
    d) d) Service Delivery Wireless Area Network
56. SASE is an acronym that represents a convergence of which two fundamental components in networking and security?
    a) Secure Access Service Edge and Software-Defined Networking
    b) Security and Service Enhancement
    c) Secure Application Service Extension and Network Gateway
    d) Secure Access and Subnet Encryption
57. What is the primary purpose of an Intrusion Detection System (IDS) in cybersecurity?
    a) To prevent unauthorized access to a network
    b) To detect and log suspicious activities and security breaches
    c) To encrypt data transmission between network devices
    d) To filter incoming and outgoing network traffic based on predefined security rules
58. Which cybersecurity solution is designed to enforce security policies and provide secure access to resources regardless of user location or device type, often leveraging cloud-based architecture?
    a) Proxy Server
    b) Jump Server
    c) SASE
    d) IPS
59. What's the primary benefit of asymmetric encryption compared to symmetric encryption?
    a) Asymmetric encryption employs a dual-key system (public and private) for communication, bolstering security.

b) Symmetric encryption relies solely on a single key for communication.
c) Asymmetric encryption is more robust in security compared to symmetric encryption.
d) It's suited for handling large data sets efficiently.

60. Which of the following categorizations pertains to the Three States of Data?
    a) Data in storage, data in transit, and data in action.
    b) Data at rest, data in motion, and data in use.
    c) Data at rest, data in transit, and data in processing.
    d) Data at rest, data in progress, and data in interaction
61. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the Internet. Which of the following BEST describes the type of certificate the company should implement?
    a) Alternative name
    b) Wildcard
    c) Self-signed
    d) Domain validation
62. Mike is the IT security analyst at getcertified4less.com. An alert has just been fired indicating a potential data exfiltration attempt in progress. He needs to act quickly to prevent sensitive information from leaving the network. Which of the following tools would be MOST effective in stopping or preventing this exfiltration attempt?
    a) NIDS
    b) DLP
    c) Firewall
    d) EDR
63. Numerous efforts have been undertaken to tamper with the lock of a high-security facility. Consequently, the security engineer has been tasked with reinforcing the access control measures. Which of the following options would most effectively fulfill the engineer's assignment?
    a) Replacing the traditional key with an RFID key
    b) Installing and monitoring a camera facing the door
    c) Setting motion-sensing lights to illuminate the door on activity
    d) Surrounding the property with fencing and gates
64. Nina is a security analyst investigating a potential data breach. Her company suspects a database containing user credentials might have been compromised. However, she cannot access the actual passwords for security reasons. Which of the following security techniques can a monitoring tool use to compare leaked data with her company's password database and identify compromised accounts without revealing the actual passwords?
    a) Encryption
    b) Multi-factor Authentication (MFA)

c) Password Management Tool
d) Hashing

65. GetCertified4Less' data security team is unsure which resource to use to benchmark their practices. Teri, an IT security consultant is brought in to advise. Which of the following resources would be MOST relevant for GetCert4Less to ensure they're compliant with European data privacy regulations?
    a) GDPR
    b) ISO
    c) NIST
    d) PCI DSS
    e) HIPAA

66. A security analyst is investigating some users who are being redirected to a fake website that resembles www. getcertified4less.org. The following output was found on the naming server of the organization:

Name	Type	Data
www.crazy.tv	A	172.17.1.17
server1	A	172.32.32.30
server2	A	172.32.32.31
file	A	172.32.32.32

Which of the following attacks has taken place?

a) A. Domain reputation
b) B. Domain hijacking
c) C. Disassociation
d) D. DNS poisoning

67. Carolyn's company is developing a groundbreaking new social media platform. To meet a tight deadline, Carolyn decides to outsource some of the back-end code development to a reputable third-party contractor. They have a good track record and come highly recommended. However, she is aware of the potential security risks involved in outsourcing code development. Which of these scenarios presents the GREATEST security concern for Carolyn's new social media platform?
    a) Intellectual property theft
    b) Elevated privileges
    c) Unknown backdoor
    d) Quality assurance
68. Once an organization has enlisted a red team to conduct simulated attacks on its security infrastructure, what actions will the blue team take upon identifying an IoC
    a) Reimage the impacted workstations.
    b) Activate runbooks for incident response.
    c) Conduct forensics on the compromised system.
    d) Conduct passive reconnaissance to gather information.
69. Michael is a security analyst on the case. A web server has been compromised and data exfiltration analysis reveals that an attacker downloaded sensitive system configuration notes. Unfortunately, the web server logs, a crucial piece of evidence, have been deleted. However, Michael discovers a clue: the stolen configuration notes were stored in the database administrator's folder on the web server itself. Which of the following attacks explains what occurred? (Choose two.)
    a) Pass-the-hash
    b) Directory traversal

c) SQL injection
d) Cross-site scripting
e) Privilege escalation
f) Request forgery

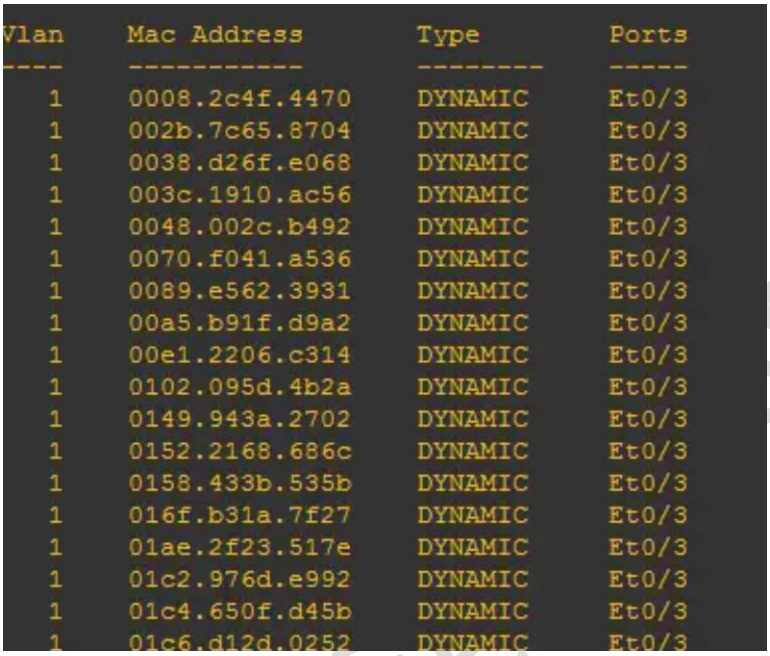
70. The Security Operations Center (SOC) of a prominent Managed Security Service Provider (MSSP) is convening to deliberate on the insights garnered from a recent protracted incident resolution. Such incidents have become increasingly frequent in recent weeks, burdening analysts with substantial time commitments due to the reliance on manual processes. Which of the following solutions should the SOC prioritize to significantly enhance its response time?
    a) Configure a Network Intrusion Detection System (NIDS) appliance utilizing a Switched Port Analyzer (SPAN).
    b) Aggregate Open-Source Intelligence (OSINT) data and systematically categorize artifacts within a centralized repository.
    c) Deploy a Security Orchestration, Automation, and Response (SOAR) platform equipped with customizable playbooks.
    d) Implement a Security Information and Event Management (SIEM) system bolstered by community-driven threat intelligence feeds.
71. Nina, a security analyst wants to fingerprint a web server. Which of the following tools will Nina MOST likely use to accomplish this task?
    a) nmap -pl-65535 192.168.0.10
    b) dig 192.168.0.10
    c) curl --head http://192.168.0.10
    d) ping 192.168.0.10
72. Carolyn is tasked with investigating the inaccuracies in the recent business impact analysis (BIA) conducted by a third-party vendor hired by her company, which operates at a headquarters notorious for unethical practices. Despite the company having multiple remote sites, the majority of its operations are centralized in one location. The BIA, known for its high accuracy, failed to accurately predict the impact of a recent incident, causing significant repercussions for the business. In her report, Carolyn must delve into the reasons behind this discrepancy. What factors contributed to the BIA's failure to foresee the true extent of the incident's impact?
    a) The vendor overlooked the organization's remote sites.
    b) The vendor was unaware of the organization's unethical practices.
    c) The vendor was unaware of some of the organization's business concepts.
    d) The vendor used the incorrect method to conduct their analysis.
73. You want to manage your passwords for different accounts to optimally secure passwords from compromise. Which of the following password management methods should you use?

a) Password vault
b) Password digest
c) Password key
d) Password generator

74. Sarah has taken out an insurance policy on her data/systems to share some of the risk with another entity. What type of risk strategy is this?
    a) Transformation
    b) Conveyance
    c) Transference
    d) Devolution
75. A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output: [SELECT *FROM user WHERE name='admin' and 'password'="" or 1=1]Which of the following is MOST likely occurring?
    a) XSS attack
    b) SQLi attack
    c) Replay attack
    d) XSRF attack
76. Which of the following is a single sign-on authentication method?
    a) CHAP
    b) IPsec
    c) EAPoL
    d) SSL
    e) Kerberos

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

77. In the wake of a recent network security incident, security analysts are meticulously combing through log data. The investigation reveals that an attacker managed to capture network traffic flowing between various workstations within the organization's network. The analysts are now focusing on the following specific log entries:



Vlan	Mac Address	Type	Ports
1	0008.2c4f.4470	DYNAMIC	Et0/3
1	002b.7c65.8704	DYNAMIC	Et0/3
1	0038.d26f.e068	DYNAMIC	Et0/3
1	003c.1910.ac56	DYNAMIC	Et0/3
1	0048.002c.b492	DYNAMIC	Et0/3
1	0070.f041.a536	DYNAMIC	Et0/3
1	0089.e562.3931	DYNAMIC	Et0/3
1	00a5.b91f.d9a2	DYNAMIC	Et0/3
1	00e1.2206.c314	DYNAMIC	Et0/3
1	0102.095d.4b2a	DYNAMIC	Et0/3
1	0149.943a.2702	DYNAMIC	Et0/3
1	0152.2168.686c	DYNAMIC	Et0/3
1	0158.433b.535b	DYNAMIC	Et0/3
1	016f.b31a.7f27	DYNAMIC	Et0/3
1	01ae.2f23.517e	DYNAMIC	Et0/3
1	01c2.976d.e992	DYNAMIC	Et0/3
1	01c4.650f.d45b	DYNAMIC	Et0/3
1	01c6.d12d.0252	DYNAMIC	Et0/3

Which of the following attacks has MOST likely occurred?

a) SQL injection
b) B. DNS spoofing
c) C. MAC flooding
d) D. ARP poisoning

78. http://example.com/viewfile?filename=myfile.txt
http://example.com/viewfile?filename=../../../../etc/passwd
Malicious filename: ../../../../etc/passwd
/var/www/html/uploads/../../../../etc/passwd

Which of the following explains these log entries?

a) SQL injection and improper input-handling attempts
b) Cross-site scripting and resource exhaustion attempts
c) Command injection and directory traversal attempts
d) Error handling and privilege escalation attempts

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

79. Match the appropriate attack and remediation from list to label the corresponding attack with its prevention.

Attack	Type of Attack	Prevention
Multiple SYN packers for Multiple sources to a server,	botnet	enable ddos protection
A connection that allows remote commands to be executed on a Client's Computer	RAT	Disable remote Access Services
a self-propagating attack that compromises a SQL database using credentials as it moves from system to system inside a network	worm	insure default passwords are changed
the attack remote monitors the user input activities to gain credentials	keylogger	implement mfa
Hidden access is established with internally developed software that bypasses account login	back door	perform code review
Payload is [lookup=$(whoami)]	command injection	input sanitization

List of Attack types	List of Preventions
RAT	Implement MFA
Worm	Disable remote access services
Botnet	Input Sanitization
Keylogger	Perform a code review
Command Injection	Enable DDOS protection
BackDoor	Insure default passwords are changed

80. Carrie wants to use hardware or software that captures packets to decode and analyze packet contents over her LAN. What is the BEST tool Carrie should use?
    a) Protocol Analyzer
    b) Patch Panel
    c) Tone Generator
    d) Fire Extinguisher

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

81. What kind of Attach is this

```
# A function to create the ".path" at the root of the installed directory
# Returns the list of affected directories
def create_dotpath(py):
  path=os.path.join(basepath,py)
  if not os.path.isdir(path):
    return
  pathfile=os.path.join(path,".path")
  debug("Generation of %s..."%pathfile)
  pathlist=[path]
  ret=[]
  for f in os.listdir(path):
    f=os.path.join(path,f)
    if f.endswith(".pth") and os.path.isfile(f):
      for l in file(f):
        l=l.rstrip('\n')
        if l.startswith('import'):
          # Do not ship lines starting with "import", they are executed! (complete WTF)
          continue
        pathlist.append(l)
        l2=os.path.join(path,l)
        pathlist.append(l2)
        ret.append(l2)
  fd=file(pathfile,"w")
  fd.writelines([l+'\n' for l in pathlist])
  fd.close()
  return ret
```

a) Backdoor
b) RAT
c) Logic Bomb
d) No Attack present
e) Rootkit
f) SQL Injection

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

82. What kind of Attach is this

```
csituser@ATXUbuntu:~$ for i in {1..100}; do echo "Carolyn"; done
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
Carolyn
```

a) Backdoor
b) RAT
c) Logic Bomb
d) No Attack present
e) Rootkit
f) SQL Injection

83. What kind of Attach is this

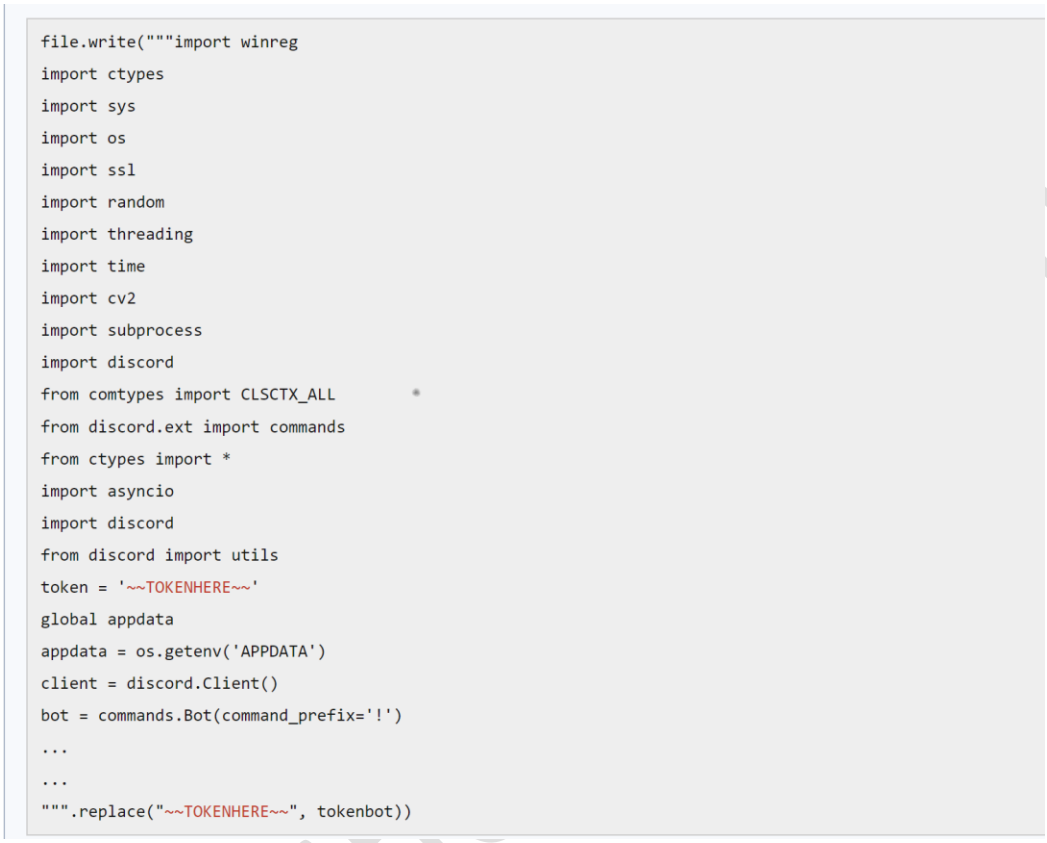
```
E:\WinIR\ScheduledTasks>schtasks /Query /FO LIST /V

HostName:                             Testsystem
TaskName:                             RVHOST.exe
Next Run Time:                        09:23:00, 4/1/2008
Status:
Last Run Time:                        Never
Last Result:                          0
Creator:                              Kim
Schedule:                             At 9:23 AM on 4/1/2008
Task To Run:                          C:\WINDOWS\system32\RVHOST.exe
Start In:                             C:\WINDOWS\system32
Comment:                              N/A
Scheduled Task State:                 Enabled
```

a) Backdoor
b) RAT
c) Logic Bomb
d) No Attack present
e) Rootkit

f) SQL Injection

84. What kind of Attach is this



```
file.write("""import winreg
import ctypes
import sys
import os
import ssl
import random
import threading
import time
import cv2
import subprocess
import discord
from comtypes import CLSCTX_ALL
from discord.ext import commands
from ctypes import *
import asyncio
import discord
from discord import utils
token = '~~TOKENHERE~~'
global appdata
appdata = os.getenv('APPDATA')
client = discord.Client()
bot = commands.Bot(command_prefix='!')
...
...
""".replace("~~TOKENHERE~~", tokenbot))
```

a) Backdoor
b) RAT
c) Logic Bomb
d) No Attack present
e) Rootkit
f) SQL Injection

85. A banner appears on a workstation during login stating that user activity may be monitored, and access is limited to authorized personnel. Clicking "OK" acknowledges these terms. What is the PRIMARY purpose of this banner?

a) To personalize the user experience
b) To collect user data for marketing purposes
c) To enforce acceptable use policies and data security
d) To welcome users to the system

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

86. Michael a security analyst is reviewing web-application logs and finds the following script:

```
<html>
<head>
  <title>CSRF Transfer</title>
</head>
<body>
  Taking the shot...

<script type='text/javascript'>

  function Call1() {
    var http;
    http = new XMLHttpRequest();

    http.open("POST", "https://jasons-bank.com/transfer.php", true);
    http.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
    http.withCredentials = "true";
    http.onreadystatechange = function() {
      var response = http.responseText;
      document.getElementById('result').innterHTML = response;
    }

  http.send('accountFrom=1234&AccountTo=6789&Amount=1000000&Submit=submit');
   }

   Call1();

</script>

</body>
</html>
```

Which of the following attacks is being observed?

a) Directory traversal
b) XSS
c) XSRF
d) On-path attack

87. Kalia, a security analyst, is inundated with multiple alerts from individual users and is striving to discern whether these diverse logins exhibit any signs of malicious activity. Her goal is to establish a baseline for regular operations and minimize the surrounding noise. Which of the following actions should the security analyst perform?

a) Adjust the data flow from authentication sources to the SIEM.
b) Disable email alerting and review the SIEM directly.
c) Adjust the sensitivity levels of the SIEM correlation engine.
d) Utilize behavioral analysis to enable the SIEM's learning mode.

88. In a corporate landscape, a sophisticated attacker has meticulously analyzed the vulnerabilities within the organization's infrastructure. After thorough reconnaissance, they've identified a cunning strategy to disrupt operations: infiltrating third-party software vendors. By compromising these vendors, the attacker can potentially gain access to sensitive data, exploit system weaknesses, and disseminate chaos within the organization. Which of the following vectors is being exploited by the attacker in this scenario?
    a) Supply chain
    b) Social media
    c) Cloud
    d) Social Engineering
89. During the software inventory report preparation, a security analyst uncovers an unauthorized program installed across the majority of the company's servers. This program shares the same code signing certificate as an application exclusive to the sales team. After removing the unauthorized program, what are the most effective mitigations the analyst should implement to enhance the security of the server environment?
    a) Revoke the code signing certificate used by both programs.
    b) Block all unapproved file hashes from installation
    c) Add the sales application file hash to the allowed list.
    d) Update the code signing certificate for the approved application
90. Nina sat down at her work computer and entered her usual password to log in. However, before she could gain access, the system prompted her for an authentication code. This two-step process is an example of Multi-Factor Authentication (MFA). Which two factors are likely being used? (Choose two)
    a) Something you know
    b) Something you have
    c) Somewhere you are
    d) Someone you know
    e) Something you are
    f) Something you can do
91. Gwendolyn, a diligent security administrator, is tasked with enhancing remote access solutions for a workforce spread across various geographical locations. Which of the following options would Gwendolyn deem as offering the utmost security for remote access? (Choose two.)

a) IPSec
b) SFTP
c) SRTP
d) LDAPS
e) S/MIME
f) SSL VPN

92. Carolyn a security administrator, who is working for a government organization, would like to utilize classification and granular planning to secure top secret data and grant access on a need-to-know basis. Which of the following access control schemas should the administrator consider?
    a) Rule-based
    b) Discretionary
    c) Mandatory
    d) Role-based
93. Eric, a security analyst, is tasked with implementing a Mobile Device Management (MDM) solution for employees using their own devices (BYOD). This MDM should prioritize two key functionalities: Securing Corporate Email and Preventing Data Loss. Which of the following would BEST meet these requirements? (Choose two.)
    a) A. Full device encryption
    b) B. Network usage rules
    c) C. Geofencing
    d) D. Containerization
    e) E. Application approve list
    f) F. Remote control
94. You're the newly appointed IT manager at a bustling e-commerce company. One morning, as you're sipping your coffee and going through your emails, when the worst happens - the servers crash. Panic ensues as you realize that critical customer data, including orders and payment information, might be lost if not recovered swiftly. Your team rushes into action, but you know you need a plan in place to ensure minimal data loss and downtime. Which of the following metrics will you rely on to determine the point in time when your organization will successfully recoup from this outage?
    a) ALE
    b) RPO
    c) MTBF
    d) ARO
95. Carrie is establishing network security measures to prevent denial-of-service attacks. She's ensuring that each message sent, such as one from Natalie, can be accurately traced back to its sender, maintaining accountability and thwarting potential denial attempts

a) Authorization
b) Encryption
c) Nonrepudiation
d) Integrity

96. Which of the following cryptographic algorithms is commonly used for securing email communications?
a) AES
b) RSA
c) DES
d) MD5

97. Which of the following is an example of physical security control?
a) Biometric authentication
b) Firewall
c) CCTV surveillance
d) Intrusion Detection System (IDS)

98. Which of the following authentication factors belongs to the category of "something you are"?
a) Password
b) Token
c) Biometric
d) Smart card

99. Which of the following best describes the principle of least privilege?
a) Users should only have access to the resources they need to perform their job functions
b) Users should be granted the highest level of access to facilitate ease of use
c) All users should have equal access to all resources on the network
d) Users should have access to all resources by default, with restrictions applied as needed

100. What is the primary purpose of an Intrusion Detection System (IDS) in a network?
a) To prevent unauthorized access to the network
b) To monitor and analyze network traffic
c) To encrypt sensitive data transmissions
d) To authenticate users accessing network resources

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

Answer

Question Number	Answer Letter(s)	Explanation
1	A	A retention policy, also called a schedule, is a collection of guidelines and procedures that an organization uses to preserve, maintain, and dispose of sensitive records by legal, regulatory, and operational requirements.
2	D	Preventive controls refer to measures and strategies implemented to prevent or reduce the likelihood of potential hazards, risks, or undesirable events from occurring within a system, process, or organization. These controls are typically put in place proactively to mitigate or eliminate risks before they can lead to negative consequences. A firewall is a preventative security control that monitors and filters network traffic based on an organization's security policies. Firewalls can be hardware or software, and they can be configured to block data from certain locations. Firewalls can prevent unauthorized access to or from a computer network, and they can also protect a computer or network from malicious or unnecessary traffic.
3	ACD	By incorporating these characteristics into the validation process, Frank can strengthen the security of his organization's Zero-Trust Network Architecture and better protect against potential threats and unauthorized access. The defining characteristic of zero-trust network architecture is that trust decisions are not based upon network location, such as IP address or MAC address.
4.	C	Honeytokens are digital resources that are purposely designed to be attractive to an attacker but signify unauthorized use. They do not serve any real purpose within your systems. However, when they are used, they trigger an alert of potentially unauthorized access. NIST
5	B	A mantrap, security mantrap portal, airlock, sally port or access control vestibule is a physical security access control system comprising a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens.

6	B	A backout plan is a strategy that outlines how to reverse and recover from changes made to a system if the changes result in undesirable outcomes. It's a safety measure that ensures data integrity and system availability. A backout plan is important because it allows organizations to quickly recover from failed changes and restore normal operations. Without a proper plan, businesses may experience revenue loss, extended downtimes, and reputational damage.
7	B	Jeremy can use netstat command to list the tcp port, if 443 port is listed there and state is established means 443 is open for outbound communication. if not it is blocked ,this is HTTPS (port 443), Jeremy's company will not be able to access secure websites.
8	D	Git is a version control tool, used to manage the development and release of source code. It does not perform any testing itself and does not have the ability to compile code, although it may be used in conjunction with other tools that accomplish those tasks. It is an important part of the change management process that has an impacted on security.
9	D	PKI is a set of policies, processes, server platforms, software and workstations used to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. The PKI includes the hierarchy of certificate authorities that allow for the deployment of digital certificates that support encryption, digital signature and authentication to meet business and security requirements NIST SP 800-95
10	ABC	June is requesting cryptographic tools that align with the hardware-based security chip requirements for strong encryption, secure boot process, system integrity, and secure key storage and generation. The cryptographic tools that fulfill these requirements include a Trusted Platform Module (TPM)is a hardware-based security chip that provides various cryptographic functions such as secure boot, cryptographic key generation, storage, and management. It ensures the integrity of the system and helps in protecting sensitive information. Hardware Security Module (HSM), is a dedicated hardware device that provides secure key

		management, encryption, and decryption services. It offers tamper resistance and protection against various attacks, making it suitable for securing cryptographic operations. Key Management System (KMS), is a software or hardware-based solution for managing cryptographic keys securely. It includes functionalities such as key generation, distribution, rotation, and revocation, ensuring that cryptographic keys are protected throughout their lifecycle. By incorporating these cryptographic tools, June can ensure strong encryption, secure boot process, system integrity, and robust key management on the server hardware platforms she's evaluating.
11	B	A distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper-evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. NIST SP 800-160 Vol. 2 Rev. 1 from NISTIR 8202, NISTIR 8301
12	A	The X.509 v2 CRL format is described and a required extension set is defined as well. An algorithm for X.509 certificate path validation is described. Supplemental information is provided describing the format of public keys and digital signatures in X.509 certificates for common Internet public key encryption algorithms such as RSA. RFC2459
13	A	A hacktivist is a hacker who uses their skills to advance a cause for political or social reasons, rather than for personal gain. The term "hacktivism" is a combination of the words "hacking" and "activism". Hacktivists often target people or organizations that represent beliefs that contradict their own. For example, a hacktivist might deface an organization's website or leak that organization's information to send a message about a cause they are promoting.
14	C	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events,

		threat scenarios, or vulnerabilities.The temporary reduction or lessening of the impact of a vulnerability or the likelihood of its exploitation. NIST SP 800-160 Vol. 2 Rev. 1 NIST SP 800-216
15	B	Threat actors, also known as cyberthreat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems. Threat actors exploit vulnerabilities in computer systems, networks and software to perpetuate various cyberattacks, including phishing, ransomware and malware attacks.
16	A	Motivation is the intent behind a cyberattack, while a threat actor is the individual or group carrying out the attack. Cybercriminals can have a variety of motivations for launching cyberattacks , including financial gain, political, economic, or military objectives, or espionage
17	C	To steal money or valuable data, To steal money or valuable data, The motivation behind 90% of attacks is about financial gain and espionage. Their attacks are intended to steal data for financial gain. Sometimes they will make that data inaccessible to the victim until they pay a hefty ransom, otherwise known as ransomware. Working alone or in a group, their primary motivation is money. Their attack arsenal is made up of phishing attacks, ransomware, malware, social engineering, and other techniques. They engage in activities like stealing sensitive information (such as credit card data, and personal information), conducting ransomware attacks, or conducting fraud. Sophos
18	B	Espionage. Nation-states, corporate competitors, or other entities may engage in cyber espionage to gather sensitive information, trade secrets, intellectual property, or government secrets for political, economic, or strategic advantage. Governments or state-sponsored entities may also conduct cyber operations to advance their national interests, engage in geopolitical maneuvering, or gather intelligence
19	B	Disrupting systems to further a political agenda, An act of cyberterrorism involves using the internet and other forms of information and communication technology to threaten or cause bodily harm to gain political or ideological power through threat or intimidation NIH.

20	C	They receive support and resources from a government entity, advanced persistent threat actors are well-resourced and engage in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion. APT objectives could include espionage, data theft, and network/system disruption or destruction.
21	C	Domain Name System (DNS) poisoning happens when fake information is entered into the cache of a domain name server, resulting in DNS queries producing an incorrect reply, sending users to the wrong website. DNS poisoning also goes by the terms “DNS spoofing” and “DNS cache poisoning.” Attackers can poison a DNS cache by tricking DNS resolvers into caching false information, with the result that the resolver sends the wrong IP address to clients, and users attempting to navigate to a website will be directed to the wrong place.cLoudflare and fortinet
22	A	A USB Data Blocker also referred to as a USB Condom, is a compact device inserted between your device and a charging port. Its purpose is to thwart data transfer while permitting charging. These blockers serve as a defense against "juice jacking," a cyber threat where a charging port is exploited for data intrusion, including malware installation or data pilferage. As awareness of such risks grows, USB data blockers have surged in popularity. They offer reassurance, especially in public charging stations like those in airports and coffee shops, which, while convenient, can pose significant risks of data compromise by cybercriminals.
23	A	A reverse proxy is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers. Reverse proxies are typically implemented to help increase security, performance, and reliability.
24	B	NXlog is a log management tool available in a free, open-source edition that would meet Riyan’s needs. NXLog is a multi-platform log management solution that allows to collect logs from various sources, filter log events, transform log data and route (forward) it to different destinations..

This practice test was created for GC4L and is intended for practice purposes only. The questions provided do not appear on the actual exam.

25	BD	Dynamic Host Configuration Protocol (DHCP) snooping is a security feature that prevents unauthorized DHCP servers from giving IP addresses to DHCP clients. Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets on a network.
26	ABD	SCADA stands for Supervisory Control and Data Acquisition and is a computerized system that uses software and hardware to gather and process data, and then control processes and equipment remotely. SCADA systems are used to control industrial and logistics processes. These systems are commonly found in facilities environments, industrial settings, manufacturing plants, energy infrastructure, and logistics operations.
27	EFG	587=SMTP Secure 993 IMAP Secure 995 POP3 Secure
28	A	The social engineering technique that seeks to exploit a person's sense of urgency is a phishing email stating a cash settlement has been awarded but will expire soon. This plays on the recipient's desire to claim the settlement before it expires, thus increasing the likelihood of them clicking on malicious links or providing sensitive information.
29	B	The Secure Shell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution.
30	C	A SQL injection attack consists of the insertion or “injection” of a SQL query via the input data from the client to the application.
31	C	Data masking or data obfuscation is the process of modifying sensitive data in such a way that it is of no or little value to unauthorized intruders while still being usable by software or authorized personnel. Data masking is a technique used to protect sensitive information by replacing, encrypting, or scrambling it with fictional but realistic data, while maintaining its usability for testing or other purposes where real data is not necessary. This process ensures that sensitive data is not exposed to unauthorized users or processes. Data masking is often used in development, testing,

		and training environments where real data should not be exposed, but realistic data is still needed for functional purposes. It helps organizations comply with privacy regulations and reduces the risk of data breaches or unauthorized access to sensitive information.
32	D	Intrusion prevention systems are the most effective security control against zero-day attacks because they can detect and block attacks even if they have not been seen before.
33	D	XSRF or CSRF stands for cross-site request forgery, which is a type of malicious attack that tricks a user into performing an unwanted action on a website or web application. XSRF is also known as one-click attack, session riding, or Sea Surf. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful XSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, XSRF can compromise the entire web application.
34	A	DLL sideloading is an attack on Windows devices in which threat actors distribute a malicious DLL together with a legitimate application that executes it. Some legitimate programs do not check the libraries that get loaded into their address space. This allows attackers to substitute a standard library with a malicious one with the same name, which a legitimate application then downloads.
35	C	Rootkits frequently collaborate with other types of malware. They constitute a collection of software utilities allowing an intruder to seize control of a computer system clandestinely. Consequently, administrators remain oblivious to the presence of the malicious program. Detection techniques involve behavioral analysis, such as monitoring anomalous activities on the system, alongside signature scanning and memory dump analysis. Regrettably, the sole recourse for eliminating a rootkit often necessitates the complete reconstruction of the compromised system.

36	B	In a replay attack, the attacker captures data packets containing sensitive information, such as login credentials, and replays them to the target system (in this case, the bank's server) in order to impersonate the legitimate user, Karla. This allows the attacker, Cody to gain unauthorized access to the Karla's account by mimicking her login session.
37	B	The most effective measure to prevent a replay attack on a login system is implementing two-factor authentication (2FA). Replay attacks involve intercepting and retransmitting data, including authentication tokens, to gain unauthorized access. 2FA adds an additional layer of security beyond just a password, making it significantly more difficult for attackers to successfully execute replay attacks. With 2FA, even if an attacker manages to capture login credentials, they would still need access to the second factor (usually a code sent to a separate device) to gain entry.
38	C	Process isolation segregates individual processes and their associated resources, thereby guaranteeing that a malfunctioning process cannot interfere with others. This directly aligns with the engineers' objective of enhancing system robustness.
39	A	Data encryption is the process of converting data from a readable format, known as plaintext, into an unreadable format, known as ciphertext, using a cryptographic algorithm and key.NIST
40	CE	The De-Militarized Zone (DMZ) feature on your router forwards all inbound traffic to a specified IP address on your local network. A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports.
41	C	Risk transference is the act of shifting risks from one area or organization to another. This is the use of contracts, insurance, disclaimers, or releases of claims to transfer the liability for the expected loss to other parties involved.
42	A	In software-defined networking (SDN), the control plane and data plane are two key components that work together to handle data. The control plane manages, routes, and processes data, while the data

		plane moves data from one system to another. The control plane also establishes and changes network topology, and performs forwarding decisions and other functions, like quality of service (QoS). The data plane is the network that switches or forwards devices handling the data packets and taking inputs from the control plane.
43	C	Infrastructure as Code (IaC) promotes consistency and repeatability in infrastructure provisioning and configuration. In a DevOps environment, where software development and deployment cycles are rapid, having a standardized and automated way to define and manage infrastructure is essential. IaC allows developers and operations teams to codify infrastructure requirements and configurations, ensuring that the same infrastructure can be easily reproduced across different environments, such as development, testing, and production.
44	C	The security considerations for microservices verus monolithic architecture are as follows: Monolithic applications present a single attack surface, whereas microservices introduce multiple points of entry. This increases the complexity of securing microservices but allows for more granular control over vulnerabilities. Microservices are inherently decoupled, reducing the likelihood of vulnerabilities propagating throughout the system. This isolation helps contain security breaches within specific services, limiting their impact on the overall application: Microservices offer greater flexibility in modifying the architecture. Each service can be updated, modified, deployed, or scaled independently, minimizing disruption and enabling swift responses to security concerns without affecting the entire system. Monolithic architectures often centralize control, which can lead to bottlenecks and single points of failure.
45	B	Serverless architecture is a software design approach that allows developers to build and run applications without managing infrastructure. In this model, developers write code, but the cloud provider manages the servers. Serverless architecture can offer greater scalability, more flexibility, and quicker time to release,

		all at a reduced cost. Making serverless architecture robust authentication and authorization, ensuring data security and integrity, rigorous monitoring and logging, and safeguarding against brute force
46	A	The inherent complexity of distributed applications presents significant security challenges. Ensuring consistent implementation of security best practices across multiple interconnected components becomes arduous. A crucial vulnerability arises from the potential entry points an attacker could exploit in such a distributed system. Additionally, establishing secure communication channels between various components while maintaining data integrity and confidentiality is a formidable task. Distributed systems' decentralized nature and reliance on network communication heighten their susceptibility to cyber threats, such as man-in-the-middle attacks, eavesdropping, and data tampering. Consequently, robust security measures, including encrypted communication protocols, access controls, and secure authentication mechanisms, become imperative to mitigate these risks and safeguard the overall system's integrity.
47	A	Cloud access security brokers (CASB) are designed to coordinate security policy enforcement across the cloud providers used by an organization. CASB is a security policy enforcement point that sits between cloud service providers and consumers and can be on-premises or cloud-based. CASBs are designed to protect an organization's data from loss, theft, or leakage, and to enforce security policies and address cloud service risks.
48	C	Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections.RFC 3748
49	B	A web application firewall(WAF) helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection.
50	A	Unified threat management (UTM) describes an information security system that provides a single point

		of protection against threats, including viruses, worms, spyware and other malware, and network attacks.A typical unified threat management (UTM) system has a firewall, malware detection and eradication, sensing and blocking of suspicious network probes, and so on. NIST
51	A	Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. Garnter
52	B	A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.
53	A	An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.
54	A	Secure access service edge (SASE) is an architecture that delivers converged network and security as a service capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access. These functions are delivered from the cloud and provided as a service by the SASE vendor.
55	B	A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that allows enterprises to leverage any combination of transport services – including MPLS, LTE, and broadband internet services – to securely connect users to applications.
56	A	Secure access service edge (SASE) is an architecture that delivers converged network and security as a service capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access. These functions are delivered

		from the cloud and provided as a service by the SASE vendor.
57	B	An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. The IDS is also a listen-only device. The IDS monitors traffic and reports results to an administrator.
58	C	Secure access service edge (SASE) is an architecture that delivers converged network and security as a service capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access. These functions are delivered from the cloud and provided as a service by the SASE vendor.
59	A	Asymmetric encryption, also known as public key cryptography, uses a public key from a public/private key pair to encrypt plaintext and then uses the corresponding private key to decrypt the ciphertext.
60	B	These terms refer to the different states that data can be in: stored or stationary (at rest), actively moving between systems (in motion), or being processed or accessed by applications or users (in use)
61	B	A wildcard certificate secures a single domain and all its subdomains. This is ideal for the company's situation as it simplifies management for a large number of subdomains under one domain. It is a special type of SSL/TLS certificate that offers a convenient and cost-effective way to secure an entire domain and all its subdomains with a single certificate.
62	B	DLP (Data Loss Prevention)solutions focus on identifying and protecting sensitive data itself, regardless of the method used for exfiltration
63	D	Fencing and gates: This creates a physical barrier and makes it harder to reach the door in the first place.
64	D	Hashing takes an input (like a password) and converts it into a unique, fixed-length string of characters called a hash value. Importantly, it's a one-way operation – you cannot recreate the original password from the hash. This allows monitoring tools to compare stolen password hashes with stored user hashes without ever

		needing the actual passwords in plain text. If a match is found, it suggests a potential leak.
65	A	General Data Protection Regulation (GDPR) compliance means that an organization meets the requirements for handling personal data as defined by the law. The GDPR is a European Union law that applies to organizations around the world and requires businesses to protect the privacy and personal data of EU citizens.
66	D	DNS poisoning involves altering DNS records to redirect users to malicious sites. In DNS poisoning, attackers manipulate the DNS records on a server.
67	C	The contractor, intentionally or unintentionally, inserts a hidden piece of code "a backdoor" that gives them unauthorized access to your platform in the future. A backdoor is a hidden or unauthorized entry point that allows an attacker to access a computer system or network without going through normal authentication procedures.
68	C	Conducting forensics on a compromised system involves systematically examining the system to determine the extent of the compromise, identify the attack vectors, gather evidence, and understand the actions taken by the attacker.
69	BE	Directory traversal, also known as path traversal or directory climbing, is a web application vulnerability that allows attackers to access restricted directories, execute commands, and view data outside of the web root folder. Directory traversal attacks can lead to privilege escalation, which is when an attacker gains elevated privileges.
70	C	SOAR stands for Security Orchestration, Automation, and Response, and it's a system of tools and services that automate cyberattack prevention and response. SOAR can help IT teams by combining efforts to address the network environment and reducing the burden on them. SOAR tools can integrate multiple components, often from different vendors, to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.
71	C	Nina would most likely use the curl --head http://192.168.0.10 command to retrieve the HTTP

		headers from the web server. This command sends a HTTP HEAD request to the specified URL and displays the headers returned by the server. By examining the headers, the analyst can gather information about the web server software and version, which helps in fingerprinting the server. "cURL" is a computer software project providing a library and command-line tool for transferring data using various network protocols. The name stands for "Client for URL"
72	A	As the remote sites also contribute to the organization's functionalities, the vendor likely overlooked them, analyzing only the main site's functions. This likely led to the inaccurate analysis.
73	C	Since a password key is a hardware-based password management tool, it provides optimum security to the password. Password key is a physical device that can be used as a hardware-based authentication method to access a system. It is plugged into a USB drive and prevents others from logging into an account, even if they have the username and password, because they do not have the password key.
74	C	Risk transference is the process of transferring liability for a loss to another party through contracts, insurance, disclaimers, or releases of claims. It's a risk management technique that allows one party to assume the liabilities of another.
75	B	SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.
76	e	Kerberos: A widely used SSO method that employs a trusted third-party server to authenticate users for various applications. Kerberos establishes a secure single sign-on environment by issuing tickets to users after successful authentication. These tickets are then used by

		applications to verify the user's identity without requiring separate logins.
77	C	MAC flooding is a cyber attack targeting switches on a local area network (LAN). It involves sending many packets with fake MAC addresses to overflow the switch's address table, causing it to become full and unable to process any legitimate traffic. Once the table becomes full, the switch will flood all packets to all ports, turning the switch into a hub and potentially causing a denial of service (DoS) condition.
78	C	Directory traversal, also known as path traversal or directory climbing, is a web application vulnerability that allows an attacker to access restricted directories and execute commands outside of the web server's root directory. An attacker discovers the application doesn't properly validate the filename. They craft a malicious filename to navigate outside the intended directory. Here's our example: Malicious filename: ../../../../etc/passwd Explanation: ../../ - This sequence moves up one directory level three times, reaching the root directory (/). /etc/passwd - This specifies the target file, the password file on Unix systems (containing sensitive information).
79	B	Multiple SYN packers for Multiple sources to a server, | Botnet |Enable DDOS Protection A connection that allows remote commands to be executed on a Client Computer|RAT|Disable remote access services a self-propagating attack that compromises a SQL database using credentials as it moves from system to system inside a network |Worm| Insure default passwords are changed the attack remote monitors the user input activities to gain credentials|Keylogger|Implemet MFA

		Hidden access is established with internally developed software that bypasses account login |BackDoor| perform a code review Payload is [lookup=$(whoami)]|Command Injection| Input Sanitization
80	A	Protocol Analyzer (examples are LeCroy and Wireshark)
81	E	Rootkit is a set of software tools that enable an unauthorized user to gain control of a computer system without being detected..
82	D	This a normal simple Bash Loop
83	C	A Logic Bomb is a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.
84	B	Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.
85	C	An Acceptable Use Policy (AUP) is a set of guidelines and rules established by organizations to define approved usage of their computing resources. This policy outlines the expectations for how employees and other authorized users should interact with these resources.
86	C	Cross-site request forgery (XSRF), also known as CSRF, is a type of attack that tricks a user into performing an unwanted action on a website or web application without their knowledge. The attack uses the victim's identity and privileges to perform the action.
87	B	Disabling email alerting means turning off notifications sent via email regarding security events or alerts. Instead of receiving these alerts in her email inbox, Kalia would directly review the Security Information and Event Management (SIEM) system. The SIEM aggregates and analyzes security data from various sources within an organization's IT infrastructure, providing a centralized platform for monitoring and managing security events. By reviewing the SIEM directly, Kalia can have a more comprehensive and real-time understanding of security incidents, allowing her

		to respond more effectively and efficiently. This approach also helps reduce the noise associated with email alerts and enables Kalia to focus on critical security events..
88	A	In this scenario, the vector being exploited is the supply chain. The supply chain refers to the network of organizations and processes involved in producing and distributing goods or services. In the context of cybersecurity, supply chain attacks occur when attackers target the suppliers or vendors of an organization rather than directly attacking the organization itself.By infiltrating third-party software vendors, the attacker can compromise the integrity of the software or services provided by these vendors.
89	A	Revoking the certificate ensures that neither the unauthorized program nor the legitimate program can leverage its validity for future installations.
90	AB	Something you know: Nina's usual password falls under this category. Something you have: The authentication code she needs likely comes from a source she possesses, like her phone or a security key.
91	AF	IPSec : Provides a robust framework for secure communication over IP networks through encryption and authentication. Gwendolyn would likely consider IPSec as a strong contender for ensuring the security of remote access. SSL VPN : SSL VPN (Secure Sockets Layer Virtual Private Network) is a widely used remote access solution that encrypts traffic between the user's device and the VPN gateway, providing secure access to internal resources over the internet. Gwendolyn might see SSL VPN as another strong option for secure remote access.
92	C	Mandatory access control (MAC) is a computer security policy that limits access to resources based on the sensitivity of the information they contain and the user's authorization.
93	DF	Containerization: This is a strong option for BYOD scenarios. It allows corporate data and applications to be isolated from personal data and applications on the device. This helps secure corporate email and prevents data loss by keeping corporate data within a secure container.

		Remote control: Remote control capabilities can be useful for managing devices, but they are not directly related to securing corporate email or preventing data loss..
94	B	Recovery Point Objective(RPO): This is the maximum tolerable period in which data might be lost due to an incident. It precisely identifies the point in time to which you must recover data after an outage to avoid significant loss. For example, if your RPO is two hours, you need to ensure that you can recover data up to that point to avoid losing critical information.
95	C	Non-repudiation assures that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
96	B	RSA (Rivest-Shamir-Adleman) is commonly used for securing email communications through encryption and digital signatures. It's asymmetric, meaning it uses a public-private key pair, making it suitable for securing communications over untrusted networks like the internet.
97	C	CCTV (Closed-Circuit Television) surveillance is a physical security control that involves the use of cameras to monitor and record activities in physical spaces. It helps deter unauthorized access and provides evidence in case of security incidents.
98	C	Biometric authentication relies on unique biological traits of individuals, such as fingerprints, iris patterns, or facial recognition. It falls under the category of "something you are" in multi-factor authentication.
99	A	The principle of least privilege dictates that users should only be granted the minimum level of access or permissions necessary to perform their job functions. This minimizes the potential impact of security breaches or insider threats by limiting the exposure of sensitive resources.
100	A, B and C	Getting to www.getcertified4less.com is as easy as ABC, pathping, traceroute, and tracert.