1. Which of the following statement holds true in terms of containers?
   1. Process-level isolation happens, a container in hence less secure
   2. Container requires more memory space
   3. Each container runs in its own OS
   4. Container is fully isolated; hence, more secure
2. In \_\_\_\_\_\_ method, event logs are arranged in the form of circular buffer.
   1. Non-wrapping method
   2. LIFO method
   3. FIFO method
   4. Wrapping method
3. Which of the following is not part of the recommended first response steps for network defenders?
   1. Extract relevant data from the suspected devices as early as possible
   2. Restrict yourself from doing the investigation
   3. Disable virus protection
   4. Do not change the state of the suspected device
4. A US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that requires a minimum of six drives but will show high fault tolerance and high speed for the data read and write operations. What RAID level will John need to choose to meet this requirement?
   1. RAID level 50
   2. RAID level 1
   3. RAID level 10
   4. RAID level 5
5. Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?
   1. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
   2. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
   3. Dan will use his public key to encrypt his mails while Alex will use Dan’s digital signature to verify the authenticity of the mails
   4. Dan will use his digital signature to sign his mails while Alex will use Dan’s public key to verify the authenticity of the mails
6. Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consults a/an

\_\_\_\_\_\_\_ for legal advice to defend them against this allegation.

* 1. PR Specialist
  2. Evidence Manager
  3. Attorney
  4. Incident Handler

1. John has implemented \_\_\_\_\_\_ in the network to restrict the number of public IP addresses in his organization to enhance the firewall filtering technique
   1. Proxies
   2. NAT
   3. DMZ
   4. VPN
2. Which of the following can be used to disallow a system/user from accessing all applications except a specific folder on a system?
   1. Certificate rule
   2. Hash rule
   3. Internet zone rule
   4. Path rule
3. To provide optimum security while enabling safe/necessary services, blocking known dangerous services, and making employees accountable for their online activity. What Internet Access policy would Brian, the network administrator, must choose?
   1. Prudent policy
   2. Paranoid policy
   3. Promiscuous policy
   4. Permissive policy
4. Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?
   1. User Account Control (UAC)
   2. Windows Security Identifier (SID)
   3. Just Enough Administration (JEA)
   4. Credentials Guard
5. Which of the following connects the SDN controller and SDN networking devices and relays information from network services to network devices such as switches and routers?
   1. Southbound API
   2. Northbound API
   3. Eastbound API
   4. Westbound API
6. Steven is a Linux system administrator at an IT company. He wants to disable unnecessary services in the system, which can be exploited by the attackers. Which among the following is the correct syntax for disabling a service?
   1. $ sudo systemctl disable [service]
   2. $ sudo system ctl disable [service]
   3. $ sudo system.ctl disable [service]
   4. $ sudo system-ctl disable [service]
7. Jason has set a firewall policy that allows only a specific list of network services and denies everything else. This strategy is known as \_\_\_\_\_\_\_\_\_.
   1. Default deny
   2. Default accept
   3. Default allow
   4. Default access
8. John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization’s network. Which of following Wireshark filter(s) will he use to locate the

TCP OS fingerprinting attempt? (Select all that apply.)

* 1. tcp.options.mss\_val<1460
  2. tcp.flags==0x2b
  3. tcp.flags==0x00
  4. tcp.options.wscale\_val==20

1. Which command is used to change the permissions of a file or directory?
   1. chmod
   2. kill
   3. systemctl
   4. rmdir
2. Which of the following indicators refers to potential risk exposure that attackers can use to breach the security of an organization?
   1. Key risk indicators
   2. Indicators of attack
   3. Indicators of compromise
   4. Indicators of exposure
3. Syslog and SNMP are the two main \_\_\_\_\_\_\_ protocols through which log records are transferred.
   1. Host-based
   2. Network-based
   3. Push-based
   4. Pull-based
4. Elden is working as a network administrator at an IT company. His organization opted for a virtualization technique in which the guest OS is aware of the virtual environment. In which it is running and communicates with the host machines for requesting resources. Identify virtualization technique implemented by Elden’s organization.
   1. Hybrid virtualization
   2. Para Virtualization
   3. Hardware-assisted virtualization
   4. Full virtualization
5. The CEO of Max Rager wants to send a confidential message regarding the new formula for

its coveted soft drink, SuperMax, to its manufacturer in Texas. However, he fears the message

could be altered in transit. How can he prevent this incident from happening and what element of the message ensures the success of this method?

* 1. Symmetric encryption; secret key
  2. Hashing; public key
  3. Hashing; hash code
  4. Asymmetric encryption; public key

1. Docker provides Platform-as-a-Service (PaaS) through \_\_\_\_\_\_\_\_\_\_ and delivers containerized software packages.
   1. OS-level virtualization
   2. Server-level virtualization
   3. Network-level virtualization
   4. Storage-level virtualization
2. A company wants to implement a data backup that allows them to encrypt the data ensuring its security as well as access it any time and from any location. What is the appropiate backup method that should be implemented?
   1. Cloud backup
   2. Hot site backup
   3. Onsite backup
   4. Offsite backup
3. Kelly is taking backups of organization’s data. Currently, she is taking backups of only those files that are created or modaified after the last backup. What type of backup is Kelly using?
   1. Full backup
   2. Differential backup
   3. Normal backup
   4. Incremental backup
4. John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide private network information. Which type of firewall service is John thinking of implementing?
   1. Packet filtering
   2. Application-level gateway
   3. Stateful multilayer inspections
   4. Circuit level gateway
5. Which of the Windows security component is responsible for controlling access of a user to Windows resources?
   1. Security Accounts Manager (SAM)
   2. Network Logon Service (Netlogon)
   3. Local Security Authority Subsystem (LSASS)
   4. Security Reference Monitor (SRM)
6. Richard has been working as a Linux system administrator at an MNC. He wants to maintain a productive and secure environment by improving the performance of the system through Linux patch management. Richard is using Ubuntu and wants to patch the Linux system manually. Which among the following command installs updates (new ones) for Debian-based Linux OSes?
   1. Sudo apt-get dist-update
   2. Sudo apt-get update
   3. Sudo apt-get dist-upgrade
   4. Sudo apt-get upgrade
7. Disaster Recovery is a
   1. Data-centric strategy
   2. Security-centric strategy
   3. Operation-centric strategy
   4. Business-centric strategy
8. A newly hired network administrator wants to assess the organization against possible risk. He notices the organization does not have \_\_\_\_\_\_ identified, which help(s) measure the level of risk of an activity.
   1. Risk matrix
   2. Risk severity
   3. Key risk indicator
   4. Risk levels
9. Who is an IR custodian?
   1. An individual who receives the initial IR alerts and leads the IR team in all the IR activities
   2. An individual responsible for the remediation and resolution of the incident that occurred
   3. An individual who makes a decision on the classifications and the severity of the incident identified
   4. An individual responsible for conveying company details after an incident
10. Sam wants to implement a network-based IDS and finalize an IDS solution that works based on pattern matching. Which type of network-based IDS is Sam implementing?
    1. Signature-based IDS
    2. Behavior-based IDS
    3. Anomaly-based IDS
    4. Stateful protocol analysis
11. John is a senior network security administrator working at a multinational company. He wants to block specific syscall from being used by container binaries. Which Linux kernel feature restricts action within the container?
    1. Usernamespace
    2. LSMs
    3. Seccomp
    4. Cgroups
12. Which Business Continuity/Disaster Recovery activity includes action taken toward resuming all services that are dependent on business-critical applications?
    1. Recovery
    2. Resumption
    3. Restoration
    4. Response
13. Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?
    1. Get-WindowsOptionalFeature –Online –FeatureName SMB1Protocol
    2. Get-WindowsOptionalFeature –Online –FeatureNames SMB1Protocol
    3. Get-WindowsOptionalFeatures –Online –FeatureNames SMB1Protocol
    4. Get-WindowsOptionalFeatures –Online –FeatureName SMB1Protocol
14. How is an “attack” represented?
    1. Asset + Threat + Vulnerability
    2. Asset + Threat
    3. Motive (goal) + method
    4. Motive (goal) + method + vulnerability
15. How is a “risk” represented?
    1. Asset + Threat + Vulnerability
    2. Asset + Threat
    3. Motive (goal) + method
    4. Motive (goal) + method + vulnerability
16. What cryptography technique can encrypt small amounts of data and applies it to digital signatures?
    1. Hashing
    2. Asymmetric encryption
    3. Digital Certificates
    4. Symmetric encryption
17. Which command list all ports available on a server?
    1. sudo ntstat -ls tunlp
    2. sudo apt netstate –ls tunlp
    3. sudo netstat –tunlp
    4. sudo apt nst –tunlp
18. Which of the following statements holds true in terms of virtual machines?
    1. VMs are light weight than containers
    2. OS-level virtualization takes place in VMs
    3. Hardware-level virtualization takes place in VMs
    4. All VMs share the host OS
19. Fargo, head of network defense at Globadyne Tech, has discovered an undesirable process in several Linux systems, which causes machines to hang every 1 hour. Fargo would like to eliminate it, what command should he execute?
    1. # update-rc.d -f [service name] remove
    2. # kill –9 [PID]
    3. # service [service name] stop
    4. # ps ax | grep [Target Process]
20. Based on which of the following registry key the Windows Event log audit configurations are recorded?
    1. HKEY\_LOCAL\_MACHINE\SYSTEM\Services\EventLog\< ErrDev >
    2. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\EventLog\< EntAppsvc >
    3. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\< Event Log >
    4. HKEY\_LOCAL\_MACHINE\CurrentControlSet\Services\EventLog\< ESENT >
21. Which among the following filter is used to detect a SYN/FIN attack?
    1. Tcp.flags==0x003
    2. Tcp.flags==0x002
    3. Tcp.flags==0x004
    4. Tcp.flags==0x001
22. How is application whitelisting different from application blacklisting?
    1. It allows execution of trusted applications in a unified environment
    2. It rejects all applications other than the allowed applications
    3. It allows execution of untrusted applications in an isolated environment
    4. It allows all applications other than the undesirable applications
23. Albert works as a Windows system administrator at an MNC. He uses PowerShell logging to identify any suspicious scripting activity across the network. He wants to record pipeline execution details as PowerShell executes?
    1. Module logging
    2. Event logging
    3. Transcript logging
    4. Script block logging
24. Which of the following security models enable strict identity verification for every user or device attempting to access the network resources?

I. Zero-trust network model II. Castle-and-Moat model

* 1. Both I and II
  2. II only
  3. None
  4. I only

1. Choose the correct order of steps to analyze the attack surface.
   1. Identify the indicators of exposure -> simulate the attack -> visualize the attack surface - > reduce the attack surface
   2. Visualize the attack surface -> identify the indicators of exposure -> simulate the attack -> reduce the attack surface
   3. Visualize the attack surface -> simulate the attack -> identify the indicators of exposure -
      * reduce the attack surface
   4. Identify the indicators of exposure -> visualize the attack surface -> simulate the attack -
      * reduce the attack surface
2. Which of the following data security technology can ensure information protection by obscuring specific areas of information?
   1. Data retention
   2. Data hashing
   3. Data encryption
   4. Data masking
3. Which Business Continuity/Disaster Recovery activity works on the assumption that the most critical processes are brought back from a remote location first, followed by the less critical functions?
   1. Resumption
   2. Restoration
   3. Recovery
   4. Response
4. Identify the attack signature technique carried out when attack signatures are contained in packet headers?
   1. Context-based signature analysis
   2. Content-based signature analysis
   3. Atomic signature-based analysis
   4. Composite signature-based analysis
5. An employee of a medical service company clicked a malicious link in an email sent by an attacker. Suddenly employees of the company are not able to access billing information or client record as it is encrypted. The attacker asked the company to pay money for gaining access to their data. Which type of malware attack is described above?
   1. Trojan
   2. Rootkits
   3. Ransomware
   4. Logic Bomb
6. Which of the following entities is responsible for cloud security?
   1. Cloud broker
   2. Both cloud consumer and provider
   3. Cloud provider
   4. Cloud consumer
7. Emmanuel works as a Windows system administrator at an MNC. He uses PowerShell to enforce the script execution policy. He wants to allow the execution of the scripts that are signed by a trusted publisher. Which of the following script execution policy settings this is?
   1. Unrestricted
   2. AllSigned
   3. RemoteSigned
   4. Restricted
8. If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings o the company’s Linux systems, which directory should he access?
   1. /etc/logrotate.conf
   2. /etc/login.defs
   3. /etc/hosts.allow
   4. /etc/crontab
9. Which of the following is true regarding any attack surface?
   1. Decrease in risk exposures increase the attack surface
   2. Decrease in vulnerabilities decease the attack surface
   3. Decrease in vulnerabilities increases the attack surface
   4. Increase in vulnerabilities decreases the attack surface
10. You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from a certain region. You suspect a DoS incident on the network. What will be your first reaction as a first responder?
    1. Make an initial assessment
    2. Avoid fear, uncertainty, and doubt
    3. Disable virus protection
    4. Communicate the incident
11. Identify the type of event that is recorded when an application driver loads successfully in Windows.
    1. Information
    2. Warning
    3. Success Audit
    4. Error
12. Which of the following is NOT an AWS Shared Responsibility Model devised by AWS?
    1. Shared Responsibility Model for Storage Services
    2. Shared Responsibility Model for Abstract Services
    3. Shared Responsibility Model for Infrastructure Services
    4. Shared Responsibility Model for Container Services
13. Simran is a network administrator at a start-up called Revolution. To ensure that neither party in the company can deny getting email notifications or any other communication, she mandates authentication before a connection establishment or message transfer occurs. What fundamental attribute of network defense is she enforcing?
    1. Non-repudiation
    2. Integrity
    3. Confidentiality
    4. Authentication
14. Henry, head of network security at Gentech, has discovered a general report template that someone has reserved only for the CEO. Since the file has to be editable, viewable, and removeable by everyone, what permission value should he set?
    1. 777
    2. 600
    3. 700
    4. 755
15. An attacker uses different types of password cracking techniques to crack the password and gain unauthorized access to a system. The attacker uses a file containing a list of commonly used passwords. They then upload this file into the cracking application that runs against the user accounts. Which of the following password cracking techniques is the attacker trying?
    1. Dictionary
    2. Bruteforce
    3. Hybrid
    4. Rainbow table
16. Blake is working on the company’s updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response. Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?
    1. Mid severity level
    2. Low severity level
    3. High severity level
    4. Extreme severity level
17. Which of the following creates passwords for individual administrator accounts and stores them in Windows AD?
    1. LSASS
    2. LAPS
    3. SAM
    4. SRM
18. A local bank wants to protect their cardholder data. Which of the following standard the bank should comply with in order to ensure the security of card holder’s data?
    1. GDPR
    2. HIPAA
    3. SOX
    4. PCI DSS
19. Daniel, who works as a network administrator, has just deployed an IDS in his organization’s network. He wants to calculate the false positive rate for his implementation. Which of the following formulas will he use calculate the false positive rate?
    1. True negative/(false negative+true positive)
    2. False negative/(false negative+true positive)
    3. False negative/(true negative+true positive)
    4. False positive/(false positive+true negative)
20. In MacOS, how can the user implement disk encryption?
    1. By enabling FileVault feature
    2. By enabling BitLocker feature
    3. By turning on Device Encryption feature
    4. By executing dm-crypt command
21. Sam, a network administrator, is using Wireshark to monitor the network traffic of the organization. He wants to detect TCP packets with no flag set to check for a specific attack attempt. Which filter will he use to view the traffic?
    1. tcp.flags==x0000
    2. tcp.flags==000x0
    3. tcp.flags==0000x
    4. tcp.flags==0x000
22. Which of the following refers to the data that is stored or processed by RAM, CPUs, or databases?
    1. Data at Rest
    2. Data is Use
    3. Data in Backup
    4. Data in Transit
23. Phishing-like attempts that present users a fake usage bill of the cloud provider is an example of a
    1. Cloud to user attack surface
    2. User to cloud attack surface
    3. User to service attack surface
    4. Cloud to service attack surface
24. Which of the following helps prevent executing untrusted and untested programs or code from untrusted or unverified third-parties?
    1. Application sandboxing
    2. Application blacklisting
    3. Application whitelisting
    4. Deployment of WAF’s
25. Byron, a new network administrator at FBI, would like to ensure that Windows PCs there are up-to-date and have less internal security flaws. What can he do?
    1. Install antivirus software and turn off unnecessary services
    2. Dedicate a partition on HDD and format the disk using NTFS
    3. Centrally assign Windows PC group policies
    4. Download and install latest patches and enable Windows Automatic Updates
26. John wants to implement a packet filtering firewall in his organization’s network. What TCP/IP later does a packet filtering firewall work on?
    1. Network interface layer
    2. Application later
    3. TCP layer
    4. IP layer
27. The \_\_\_\_\_\_ mechanism works on the basis of a client-server model.
    1. Host-based
    2. Push-based
    3. Network-based
    4. Pull-based
28. Assume that you are working as a network defender at the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to main server. How will you prioritize these two incidents?
    1. Based on a first come first served basis
    2. Based on approval from management
    3. Based on a potential technical effect of the incident
    4. Based on the type of response needed for the incident

1. John, a network administrator, is configuring Amazon EC2 cloud service for his organization. Identify the type if cloud service modules his organization adopted.
   1. Storage-as-a-Service (STaaS)
   2. Platform-as-a-Service (PaaS)
   3. Infrastructure-as-a-Service (IaaS)
   4. Software-as-a-Service (SaaS)
2. Which subdirectory in /var/log directory stores information related to Apache web server?
   1. /var/log/maillog/
   2. /var/log/apachelog/
   3. /var/log/httpd/
   4. /var/log/lighttpd/
3. Nancy is working as a network defender for a small company. Management wants to implement a RAID storage for their organization. They want to use the appropriate RAID level for their backup plan that will satisfy the following requirements: 1) Parity check to store all the information about the data in multiple drives, 2) Help reconstruct the data during downtime, 3) Process the data at a good speed, and 4) Should not be expansive. The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements. What RAID level will she suggest?
   1. RAID 3
   2. RAID 0
   3. RAID 1
   4. RAID 10
4. John is working as a network defender at a well-reputed multinational company. He wanted to implement security that can help him identify any future attacks that can be targeted toward his organization and take appropriate security measures and action beforehand to defend against them. Which one of the following security defense techniques should he implement?
   1. Retrospective security approach
   2. Proactive security approach
   3. Preventive security approach
   4. Reactive security approach
5. Ryan works as a network security engineer at an organization the recently suffered an attack. As a countermeasure, Ryan would like to obtain more information about the attacker and chooses to deploy a honeypot into the organizations production environment called Kojoney. Using this honeypot, he would like to emulate the network vulnerability that was attacked previously. Which type of honeypot is he trying to implement?
   1. Low-interaction honeypots
   2. Research honeypots
   3. Pure honeypots
   4. High-interaction honeypots
6. Which of the following helps in viewing account activity and events for supported services made by AWS?
   1. AWS CloudHSM
   2. AWS Certificate Manager
   3. AWS CloudFormation
   4. AWS CloudTrail
7. Management decides to implement a risk management system to reduce and maintain the organization’s risk to an acceptable level. Which of the following is the correct order in risk management phase?
   1. Risk assessment, risk treatment, risk monitoring and review, risk identification
   2. Risk treatment, risk monitoring and review, risk identification, risk assessment
   3. Risk identification, risk assessment, risk treatment, risk monitoring and review
   4. Risk identification, risk assessment, risk monitoring and review, risk treatment
8. How can a WAF validate traffic before it reaches a web application?
   1. It uses a sandboxing filtering technique
   2. It uses a role-based filtering technique
   3. It uses an access-based filtering technique
   4. It uses a rule-based filtering technique
9. Which of the following provides a set of voluntary recommended cyber security features to include in network-capable IoT devices?
   1. FGMA
   2. NIST
   3. GCMA
   4. GLBA
10. Which of the following attack surface increase when you keep USB ports enabled on your laptop unnecessarily?
    1. Network attack surface
    2. Human attack surface
    3. Physical attack surface
    4. Software attack surface
11. Which among the following tools can help in identifying IoEs (Indicator of Exposures) to evaluate human attack surface?
    1. Amass
    2. Skybox
    3. securiCAD
    4. SET
12. Which of the following refers to a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization?
    1. Threat
    2. Risk
    3. Attack
    4. Vulnerability
13. Ross manages 30 employees and only 25 computers in the organization. The network the company uses is peer-to-peer. Ross configures access control measures allowing the employees to set their own control measures for their files and folders. Which access control did Ross implement?
    1. Non-discretionary access control
    2. Role-based access control
    3. Discretionary access control
    4. Mandatory access control
14. Peter works as a network administrator at an IT company. He wants to avoid exploitation of the cloud, particularly Azure services. Which of the following is a group of PowerShell scripts designed to help the network administrator understand how attacks happen and help them protect the cloud?
    1. MicroBurst
    2. POSH-Sysmon
    3. Sysmon
    4. SecurityPolicyDsc
15. Mark is monitoring the network traffic on his organization's network. He wants to detect TCP and UDP ping sweeps on his network. Which type of filter will be used to detect this?
    1. tcp.dstport==7 and udp.srcport==7
    2. tcp.srcport==7 and udp.srcport==7
    3. tcp.dstport==7 and udp.dstport==7
    4. tcp.srcport==7 and udp.dstport==7
16. In \_\_\_\_\_\_\_\_ mechanism, the system or application sends log records either on the local disk or over the network.
    1. Push-based
    2. Host-based
    3. Pull-based
    4. Network-based
17. Which type of firewall consists of three interfaces and allows further subdivision of the system based on specific security objectives of the organization?
    1. Unscreened subnet
    2. Screened subnet
    3. Bastion host
    4. Multi-homed firewall
18. Which of the following defines the extent to which an interruption effects normal business operation and the amount of revenue lost due to that interruption?
    1. RPO
    2. RTO
    3. RSP
    4. RFO
19. James working as a network administrator at a reputed company situated in California, USA. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?
    1. icmp.type==8 and icmp.type==0
    2. icmp.type==8 or icmp.type==16
    3. icmp.type==0 and icmp.type==16
    4. icmp.type==8 or icmp.type==0
20. If an organization has decided to consume PaaS Cloud service model, then identify the organization’s responsibility that they need to look after based on shared responsibility model.
    1. Data, interfaces, application, middleware, OS, VM, virtual network, hypervisors, processing and memory, data storage, network interfaces, facilities and data centers, etc.
    2. Data, interfaces, etc.
    3. Data, interfaces, application, middleware, OS, VM, virtual network, etc.
    4. Data, interfaces, application, etc.
21. Identify the virtualization level that creates a massive pool of storage areas for different virtual machines running on the hardware
    1. Storage device virtualization
    2. Server virtualization
    3. Fabric virtualization
    4. File system virtualization
22. Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the \_\_\_\_\_\_\_\_\_

authentication technique to satisfy the request.

* 1. Biometric
  2. Single-sign-on
  3. Smart card authentication
  4. Two-factor authentication

1. Which type of attack is used to hack an IoT device and direct large amounts of network traffic toward a web server, resulting in overloading the server with connections and preventing any new connections?
   1. XSS
   2. Sniffing
   3. DDoS
   4. XCRF
2. Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?
   1. Mitigation
   2. Verification
   3. Remediation
   4. Assessment
3. Damian is the chief security officer of Enigma Electronics. To block intruders and prevent any environmental accidents, he needs to set a two-factor authenticated keypad lock at the entrance, rig a fire suppression system, and link any video cameras at various corridors to view the feeds in the surveillance room. What layer of network defense-in-depth strategy is he trying to follow?
   1. Physical
   2. Perimeter
   3. Policies and procedures
   4. Host
4. Leslie, the network administrator of Livewire Technologies, has been recommending multiplayer inspection firewalls to deploy the company's infrastructure. What layers of the TCP/IP model can it protect?
   1. IP, application, and network interface
   2. Application, IP, and network interface
   3. Network interface, TCP, and IP
   4. Application, TCP, and IP
5. Which of the following is an example of MAC model?
   1. Clark-Beason integrity model
   2. Bell-LaPadula model
   3. Access control matrix model
   4. Chinese Waterfall model
6. Which of the following things need to be identified during attack surface visualization?
   1. Authentication, authorization, and auditing in networks
   2. Attacker’s tools, techniques, and procedures
   3. Assets, topologies, and policies of the organization
   4. Regulatory frameworks, standards and, procedures for organizations
7. How can one identify the baseline for normal traffic?
   1. When the FIN flag appears at the beginning and SYN flag appears at the end of the connection
   2. When the ACK flag appears at the beginning and RST flag appears at the end of the connection
   3. When the SYN flag appears at the beginning and FIN flag appears at the end of the connection
   4. When RST flag appears at the beginning and the ACK flag appears at the end of the connection