Important notices:

- I passed the exam. These are the questions that I experienced in the exam. However, I'm not sure if your exam will be composed of these questions as well!
  You have the choice to study them on your responsibility.

- More than **90%** of the questions in this document are correctly answered — Still, **10%** of questions with wrong answers. I couldn't recognize them. You may try to correct them and update the document yourself.

- Passing score could be **70%** or **79%** or between them.

Which encryption algorithm is used by WPA3 encryption?

a. AES-GCMP 256
b. RC4
c. AES-CCMP
d. RC4, TKIP

John is the Vice-President of a BPO. He wants to implement a policy allowing employees to use and manage devices purchased by the organization but restrict the use of the device for business use only. Which among the following policies does John want to implement?

a. CYOD policy
b. COBO policy
c. BYOD policy
d. COPE policy

Which of the following provides enhanced password protection, secured IoT connections, and encompasses stronger encryption techniques?

a. WPA
b. WEP
c. WPA3
d. WPA2

Which of the following is a Windows in-built feature that provides filesystem-level encryption in the OS (starting from Windows 2000), except the Home version of Windows?

a. FileVault
b. EFS
c. Disk Utility
d. BitLocker

Which risk management phase helps in establishing context and quantifying risks?

a. Risk treatment
b. Risk identification
c. Risk assessment
d. Risk review

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 the private network information. Which type of firewall service is John thinking of implementing?

a. Application-level gateway
b. Packet filtering
c. Circuit level gateway
d. Stateful multilayer inspection

Ross manages 30 employees and only 25 computers in the organization. The network the company uses is a 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?

a. Role-based access control
b. Non-discretionary access control
c. Discretionary access control
d. Mandatory access control

Which among the following tools can help in identifying IoEs to evaluate human attack surface?

a. Skybox
b. securiCAD
c. SET
d. Amass

Based on which of the following registry keys, the Windows Event log audit configurations are recorded?

a. HKEY_LOCAL_MACHINE\SYSTEM\Services\EventLog\ < ErrDev >
b. HKEY_LOCAL_MACHINE\CurrentControlSet\Services\EventLog\ < ESENT >
c. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ EventLog\ < EntAppsvc >
d. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ < Event Log >

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 deletable by everyone, what permission value should he set?

a. 600
b. 777
c. 755
d. 700

Which among the following is used by anti-malware systems and threat intelligence platforms to spot and stop malicious activities at an initial stage?

a. Indicators of attack
b. Indicators of exposure
c. Key risk indicators
d. Indicators of compromise

Which of the following statements holds true in terms of virtual machines?

a. VMs are light weight than containers
b. Hardware-level virtualization takes place in VMs
c. All VMs share the host OS (not sure)
d. OS-level virtualization takes place in VMs

According to standard IoT security practice, IoT Gateway should be connected to a _____.

a. Secure router
b. Router that is connected to internal servers
c. Router that is connected to other subnets
d. Border router

How is the chip-level security of an IoT device achieved?

a. Keeping the device on a flat network
b. Changing the password of the router
c. Closing insecure network services
d. Encrypting JTAG interface

Michelle is a network security administrator working at a multinational company. She wants to provide secure access to corporate data (documents, spreadsheets, email, schedules, presentations, and other enterprise data) on mobile devices across organizations networks without being slowed down and also wants to enable easy and secure sharing of information between devices within an enterprise. Based on the above-mentioned requirements, which among the following solution should Michelle implement?

a. MCM
b. MAM
c. MDM
d. MEM

Maximus Tech is a multinational company that uses Cisco ASA Firewalls for their systems. Jason is the one of the members of the team that checks the logs at Maximus Tech. As a part of his job, he is going through the logs and he came across a firewall log that looks like this:

May 06 2018 21:27:27 asa 1: % ASA -5 â€“ 11008: User â€˜enable_15â€™ executed the â€˜configure termâ€™ command

Based on the security level mentioned in the log, what did Jason understand about the description of this message?

a. Informational message
b. Normal but significant message
c. Warning condition message
d. Critical condition message

Which firewall technology can filter application-specific commands such as GET and POST requests?

a. Stateful multi-layer inspection
b. Circuit-level gateways
c. Application proxy
d. Application-level gateways

Leslie, the network administrator of Livewire Technologies, has been recommending multilayer inspection firewalls to deploy the company's infrastructure. What layers of the TCP/IP model can it protect?

a. Application, IP, and network interface
b. IP, application, and network interface
c. Network interface, TCP, and IP
d. Application, TCP, and IP

Which firewall technology can be implemented in all (application, session, transport, network, and presentation) layers of the OSI model?

a. Circuit-level gateway
b. Packet filtering
c. Network address translation
d. VPN

In _____ mechanism, the system or application sends log records either on the local disk or over the network

a. Network-based
b. Host-based
c. Push-based
d. Pull-based

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?

Hashing; public key

Asymmetric encryption; public key

Symmetric encryption; secret key

Hashing; hash code

Which of the following statement holds true in terms of containers?

a. Process-level isolation happens; a container in hence less secure
b. Each container runs in its own OS
c. Container requires more memory space
d. Container is fully isolated; hence, more secure

Which of the following data security technology can ensure information protection by obscuring specific areas of information?

a. Data encryption
b. Data hashing
c. Data retention
d. Data masking

What defines the maximum time period an organization is willing to lose data during a major IT outage event?

a. RTO
b. RPO
c. DR
d. BC

Identify the correct order for a successful black hat operation.

a. Reconnaissance, Gaining Access, Scanning, Maintaining Access, and Covering Tracks
b. Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks
c. Scanning, Reconnaissance, Gaining Access, Maintaining Access and Covering Tracks
d. Reconnaissance, Scanning, Gaining Access, Covering Tracks, and Maintaining Access

---

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?

a. Hybrid
b. Dictionary
c. Rainbow table
d. Bruteforce

Which scan attempt can penetrate through a router and a firewall that filter incoming packets with particular flags set and is not supported by Windows?

a. ARP scan attempt
b. PING sweep attempt
c. TCP full connect scan attempt
d. TCP null scan attempt

WPA encryption in a wireless network uses _____ encryption protocol and a/an_____ integrity check.

a. EAP, CRC-32
b. CCMP, CRC-32
c. CCMP, AES-based
d. TKIP, 64-bit MIC

Which among the following options represents professional hackers with an aim of attacking systems for profit?

a. Script kiddies
b. Organized hackers
c. Cyber terrorists
d. Hacktivists

Implementing access control mechanisms, such as a firewall, to protect the network is an example of which of the following network defense approach?

a. Retrospective approach
b. Reactive approach
c. Preventive approach
d. Proactive approach

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 consulted a/an _____ for legal advice to defend them against this allegation.

a. Evidence Manager
b. Incident Handler
c. Attorney
d. PR Specialist

Which type of modulation technique is used in local area wireless networks (LAWNs)?

a. DSSS
b. MIMO-OFDM
c. FHSS
d. OFDM

A local bank wants to protect their cardholder data. Which standard should the bank comply with in order to ensure security of this data?

a. GDPR
b. PCI DSS
c. SOX
d. HIPAA

Which of the following provides a set of voluntary recommended cyber security features to include in network-capable IoT devices?

a. NIST
b. FGMA
c. GCMA
d. GLBA

John is working as a network defender at a well-reputed multinational company. He wants to implement security that can help him identify any future attacks that can be targeted toward his organization and take appropriate security measures and actions beforehand to defend against them. Which one of the following security defense techniques should he implement?

a. Retrospective security approach
b. Reactive security approach
c. Proactive security approach
d. Preventive security approach

How is a "risk" represented?

a. Asset + threat + vulnerability
b. Motive (goal) + method
c. Motive (goal) + method + vulnerability
d. Asset + threat

Ivan needs to pick an encryption method that is scalable even though it might be slower. He has settled on a method that works where one key is public and the other is private. What encryption method did Ivan settle on?

a. Ivan settled on the private encryption method.
b. Ivan settled on the hashing encryption method.
c. Ivan settled on the asymmetric encryption method.
d. Ivan settled on the symmetric encryption method.

Clement is the CEO of an IT firm. He wants to implement a policy allowing employees with a preapproved set of devices from which the employees choose devices (laptops, smartphones, and tablets) to access company data as per the organization's access privileges. Which among the following policies does Clement want to enforce?

a. CYOD policy
b. COBO policy
c. BYOD policy
d. COPE policy

Which of the following is a database encryption feature that secures sensitive data by encrypting it in client applications without revealing the encrypted keys to the data engine in MS SQL Server?

a. Allow Encrypted
b. Always Encrypted
c. IsEncrypted Enabled
d. NeverEncrypted disabled

How can a WAF validate traffic before it reaches a web application?

a. It uses an access-based filtering technique
b. It uses a role-based filtering technique
c. It uses a sandboxing filtering technique
d. It uses a rule-based filtering technique

Which firewall technology provides the best of both packet filtering and application-based filtering and is used in Cisco Adaptive Security Appliances?

a. VPN
b. Network address translation
c. Stateful multilayer inspection
d. Application-level gateway

Which of the following is an example of MAC model?

a. Windows Admin Center
b. Access control matrix model
c. Clark-Beason integrity model
d. Bell-LaPadula model

What should an administrator do while installing a sniffer on a system to listen to all data transmitted over the network?

a. Set the system's NIC to managed mode
b. Set the system's NIC to ad-hoc mode
c. Set the system's NIC to master mode
d. Set the system's NIC to promiscuous mode

John is a senior network security administrator working at a multinational company. He wants to block specific syscalls from being used by container binaries. Which Linux kernel feature restricts actions within the container?

a. Cgroups
b. LSMs
c. Seccomp
d. Userns

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?

a. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
b. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol
c. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol
d. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

---

Who is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization?

a. Chief Information Officer (CIO)
b. IT security practitioners
c. Senior management
d. Business and functional managers

Which of the following refers to the clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an organization's infrastructure?

a. Indicators of compromise
b. Key risk indicators
c. Indicators of attack
d. Indicators of exposure

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 systems through Linux patch management. Richard is using Ubuntu and wants to patch the Linux systems manually. Which among the following command installs updates (new ones) for Debian-based Linux OSes?

a. sudo apt-get dist-update
b. sudo apt-get upgrade
c. sudo apt-get dist-upgrade
d. sudo apt-get update

How is application whitelisting different from application blacklisting?

a. It allows execution of trusted applications in a unified environment
b. It rejects all applications other than the allowed applications
c. It allows all applications other than the undesirable applications
d. It allows execution of untrusted applications in an isolated environment

---

Which of the following characteristics represents a normal TCP packet?

a. The destination address is a broadcast address
b. SYN and FIN bits are set
c. Source or destination port is zero
d. FIN ACK and ACK are used in terminating the connection

Rosa is working as a network defender at Linda Systems. Recently, the company migrated from Windows to MacOS. Rosa wants to view the security related logs of her system, where can she find these logs?

a. /private/var/log
b. /Library/Logs/Sync
c. ~/Library/Logs
d. /var/log/cups/access_log

Which type of information security policy addresses the implementation and configuration of technology and user behavior?

a. System-specific security policy
b. Issue-specific security policy
c. Enterprise information security policy
d. Acceptable use policy

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?

a. $ sudo system.ctl disable [service]
b. $ sudo system ctl disable [service]
c. $ sudo system-ctl disable [service]
d. $ sudo systemctl disable [service]

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 setting this?

a. RemoteSigned
b. AllSigned
c. Unrestricted
d. Restricted

Which of the following filters can be used to detect UDP scan attempts using Wireshark?

a. icmp.type==8 or icmp.type==0
b. icmp.type==3 and icmp.code==3
c. icmp.type==13
d. icmp.type==15

In _____method, windows event logs are arranged in the form of a circular buffer.

a. Wrapping method
b. Out-of Band Method
c. Overwriting Method
d. Non-wrapping method

Who oversees all the incident response activities in an organization and is responsible for all actions of the IR team and IR function?

a. Attorney
b. PR specialist
c. IR officer
d. IR custodians

Which firewall can a network administrator use for better bandwidth management, deep packet inspection, and stateful inspection?

a. Stateful multi-layer inspection firewall
b. Network address translation
c. Next-generation firewall
d. Circuit-level gateway firewall

Oliver is a Linux security administrator at an MNC. An employee named Alice has resigned from his organization and Oliver wants to disable this user in Ubuntu. Which of the following commands can be used to accomplish this?

a. usermod -L alice
b. usermod -M alice
c. usermod -J alice
d. usermod -K alice

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?

a. Low severity level
b. Extreme severity level
c. High severity level
d. Mid severity level

Which of the following is true regarding any attack surface?

a. Decrease in vulnerabilities decreases the attack surface
b. Decrease in risk exposures increases the attack surface
c. Decrease in vulnerabilities increases the attack surface
d. Increase in vulnerabilities decreases the attack surface

Which type of risk treatment process includes not allowing the use of laptops in an organization to ensure its security?

a. Risk avoidance
b. Mitigate the risk
c. Eliminate the risk
d. Reduce the risk

Hacktivists are threat actors, who can be described as _____.

a. People motivated by religious beliefs
b. People motivated by monetary gains
c. Disgruntled/terminated employees
d. People having political or social agenda

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

a. Both I and II
b. None
c. II only
d. I only

Which of following are benefits of using IoT devices in IoT-enabled environments? I. IoT device can be connected anytime II. IoT device can be connected at any place III. IoT devices connected to anything

a. I
b. II
c. I , II, and III
d. I and II

Which of the following is a drawback of traditional perimeter security?

a. Traditional firewalls are static in nature
b. Traditional firewalls are dynamic in nature
c. Traditional VPNs follow identity-centric instead of trust-based network-centric approach
d. Traditional perimeter security is identity-centric

Which of the following filters can be applied to detect an ICMP ping sweep attempt using Wireshark?

a. icmp.type==15
b. icmp.type==17
c. icmp.type==8
d. icmp.type==13

Which RAID level system provides very good data performance but does not offer fault tolerance and data redundancy?

a. RAID level 1
b. RAID level 0
c. RAID level 5
d. RAID level 3

Which type of training can create awareness among employees regarding compliance issues?

a. Physical security awareness training
b. Training on data classification
c. Social engineering awareness training
d. Security policy training

Which of the following technologies can be used to leverage zero-trust model security?

a. Software-defined perimeter (SDP)
b. Software-defined networking (SDN)
c. Network virtualization (NV)
d. Network function virtualization (NFV)

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?

a. 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.
b. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
c. 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.
d. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.

Which form of access control is trust centric?

a. Application sandboxing
b. Application blacklisting
c. Application patch management
d. Application whitelisting

How can an administrator detect a TCP null scan attempt on a UNIX server by using Wireshark?

a. By applying the filter tcp.flags==0x002
b. By applying the filter tcp.flags==0x003
c. By applying the filter tcp.flags==0x000
d. By applying the filter tcp.flags==0x004

Which type of antenna is based on the principle of a satellite dish and can pick up Wi-Fi signals from a distance of ten miles or more?

a. Omnidirectional antenna
b. Parabolic Grid antenna
c. Yagi antenna
d. Directional antenna

Which phase of incident response process involves collection of incident evidence and sending them to forensic department for further investigation?

a. Eradication
b. Incident recording and assignment
c. Preparation for incident response
d. Incident containment

Katie has implemented a RAID level that splits data into blocks and evenly writes the data to multiple hard drives but does not provide data redundancy. This type of RAID level requires a minimum of _____ in order to setup.

a. Six drives
b. Three drives
c. Two drives
d. Four drives

Identify the method involved in purging technique of data destruction.

a. Incineration
b. Wiping
c. Degaussing
d. Overwriting

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 expensive. The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements. What RAID level will she suggest?

a. RAID 3
b. RAID 0
c. RAID 1
d. RAID 10

Disaster Recovery is a

a. Data-centric strategy.
b. Security-centric strategy.
c. Business-centric strategy.
d. Operation-centric strategy.

Which of the following indicators are discovered through an attacker's intent, their end goal or purpose, and a series of actions that they must take before being able to successfully launch an attack?

a. Indicators of exposure
b. Indicators of compromise
c. Indicators of attack
d. Key risk indicators

John has been working as a network administrator at an IT company. He wants to prevent misuse of accounts by unauthorized users. He wants to ensure that no accounts have empty passwords. Which of the following commands does John use to list all the accounts with an empty password?

a. # awk -E: '($2 == "") {print}' /etc/shadow
b. # awk -C: '($2 == "") {print}' /etc/shadow
c. # awk -D: '($2 == "") {print}' /etc/shadow
d. # awk -F: '($2 == "") {print}' /etc/shadow

Mark is monitoring the network traffic on his organizationâ€™s network. He wants to detect TCP and UDP ping sweeps on his network. Which type of filter will be used to detect this?

a. tcp.srcport==7 and udp.srcport==7
b. tcp.srcport==7 and udp.dstport==7
c. tcp.dstport==7 and udp.dstport==7
d. tcp.dstport==7 and udp.srcport==7

Who offers formal experienced testimony in court?

a. Evidence documenter
b. Expert witness
c. Attorney
d. Incident analyzer

Which type of firewall consists of three interfaces and allows further subdivision of the systems based on specific security objectives of the organization?

a. Unscreened subnet
b. Multi-homed firewall
c. Bastion host
d. Screened subnet

Which of the following helps in viewing account activity and events for supported services made by AWS?

a. AWS CloudHSM
b. AWS CloudFormation
c. AWS CloudTrail
d. AWS Certificate Manager

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 the virtualization technique implemented by Elden's organization.

a. Hybrid virtualization
b. Para virtualization
c. Hardware-assisted virtualization
d. Full virtualization

Which of the following is a data destruction technique that protects the sensitivity of information against a laboratory attack where an unauthorized individual uses signal processing recovery tools in a laboratory environment to recover the information?

a. Disposal
b. Purging
c. Destroying
d. Clearing

Which category of suspicious traffic signatures includes SYN flood attempts?

a. Denial of Service
b. Informational
c. Reconnaissance
d. Unauthorized access

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, including variable initialization and command invocations. Which PowerShell logging component records pipeline execution details as PowerShell executes?

a. Script block logging
b. Module logging
c. Transcript logging
d. Event logging

Which of the following attack surfaces increase when you keep USB ports enabled on your laptop unnecessarily?

a. Human attack surface
b. Network attack surface
c. Physical attack surface
d. Software attack surface

Docker provides Platform-as-a-Service (PaaS) through _____ and delivers containerized software packages

a. Storage-level virtualization
b. Network-level virtualization
c. OS-level virtualization
d. Server-level virtualization

Identify the type of event that is recorded when an application driver loads successfully in Windows.

a. Success Audit
b. Warning
c. Error
d. Information

Who is responsible for conveying company details after an incident?

a. IR manager
b. IR officer
c. PR specialist
d. IR custodians

James is a network administrator working at a student loan company in Minnesota. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company, schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails. What should James use?

a. James could use PGP as a free option for encrypting the company's emails.
b. James can use MD5 algorithm to encrypt all the emails.
c. James should utilize the free OTP software package.
d. James can enforce mandatory HTTPS in the email clients to encrypt emails.

Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?

a. Just Enough Administration (JEA)
b. User Account Control (UAC)
c. Windows Security Identifier (SID)
d. Credential Guard

In MacOS, how can the user implement disk encryption?

a. By turning on Device Encryption feature
b. By executing dm-crypt command
c. By enabling FileVault feature
d. By enabling BitLocker feature

Which of the following need to be identified during attack surface visualization?

a. Regulatory frameworks, standards, and procedures for organizations
b. Assets, topologies, and policies of the organization
c. Attacker's tools, techniques, and procedures
d. Authentication, authorization, and auditing in networks

What represents the ability of an organization to respond under emergency in order to minimize the damage to its brand name, business operation, and profit?

a. Crisis management
b. Incident management
c. Emergency management
d. Disaster recovery

What enables an organization to analyze, identify, and rectify hazards and prevent future recurrence in business continuity management?

a. Business recovery
b. Incident management
c. Emergency management
d. Crisis management

Which of the following entities is responsible for cloud security?

a. Cloud consumer
b. Both cloud consumer and provider
c. Cloud provider
d. Cloud broker

Which subdirectory in /var/log directory stores information related to Apache web server?

a. /var/log/lighttpd/
b. /var/log/apachelog/
c. /var/log/maillog/
d. /var/log/httpd/

A company wants to implement a data backup method that allows them to encrypt the data ensuring its security as well as access it at any time and from any location. What is the appropriate backup method that should be implemented?

a. Onsite backup
b. Offsite backup
c. Hot site backup
d. Cloud backup

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 the main server. How will you prioritize these two incidents?

a. Based on a potential technical effect of the incident
b. Based on approval from management
c. Based on a first come first served basis
d. Based on the type of response needed for the incident

Which of the following creates passwords for individual administrator accounts and stores them in Windows AD?

a. SRM
b. SAM
c. LSASS
d. LAPS

Kelly is taking backups of the organizationâ€™s data. Currently, she is taking backups of only those files that are created or modified after the last backup. What type of backup is Kelly using?

a. Full backup
b. Incremental backup
c. Normal backup
d. Differential backup

Syslog and SNMP are the two main _____ protocols through which log records are transferred.

a. Push-based
b. Host-based
c. Pull-based
d. Network-based

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?

a. Integrity
b. Authentication
c. Non-repudiation
d. Confidentiality

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?

a. Westbound API
b. Southbound API
c. Eastbound API
d. Northbound API

In _____method, event logs are arranged in the form of a circular buffer.

a. Non-wrapping method
b. FIFO method
c. Wrapping method
d. LIFO method

Which of the following can be used to disallow a system/user from accessing all applications except a specific folder on a system?

a. Hash rule
b. Path rule
c. Internet zone rule
d. Certificate rule

Which of the following is not part of the recommended first response steps for network defenders?

a. Restrict yourself from doing the investigation
b. Disable virus protection
c. Extract relevant data from the suspected devices as early as possible
d. Do not change the state of the suspected device

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?

a. Risk
b. Attack
c. Vulnerability
d. Threat

Which command list all ports available on a server?

a. sudo apt nst -tunlp
b. sudo ntstat -ls tunlp
c. sudo apt netstate -ls tunlp
d. sudo netstat -tunlp

Which of the following is NOT an AWS Shared Responsibility Model devised by AWS?

a. Shared Responsibility Model for Storage Services
b. Shared Responsibility Model for Container Services
c. Shared Responsibility Model for Abstract Services
d. Shared Responsibility Model for Infrastructure Services

Which BC/DR activity includes action taken toward resuming all services that are dependent on business-critical applications?

a. Restoration
b. Resumption
c. Response
d. Recovery

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?

Make an initial assessment

Avoid fear, uncertainty, and doubt

Communicate the incident

Disable virus protection

Which of the following indicators refers to potential risk exposures that attackers can use to breach the security of an organization?

a. Indicators of attack
b. Indicators of compromise
c. Key risk indicators
d. Indicators of exposure

The _____ mechanism works on the basis of a client-server model.

a. Pull-based
b. Push-based
c. Network-based
d. Host-based

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?

a. Extreme severity level
b. Mid severity level
c. High severity level
d. Low severity level

Which of the following defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption?

a. RPO
b. RSP
c. RTO
d. RFO

Which of the Windows security component is responsible for controlling access of a user to Windows resources?

a. Security Accounts Manager (SAM)
b. Local Security Authority Subsystem (LSASS)
c. Network Logon Service (Netlogon)
d. Security Reference Monitor (SRM)

How can one identify the baseline for normal traffic?

a. When the RST flag appears at the beginning and the ACK flag appears at the end of the connection
b. When the ACK flag appears at the beginning and the RST flag appears at the end of the connection
c. When the FIN flag appears at the beginning and the SYN flag appears at the end of the connection
d. When the SYN flag appears at the beginning and the FIN flag appears at the end of the connection

---

If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings on the companyâ€™s Linux systems, which directory should he access?

a. /etc/hosts.allow
b. /etc/crontab
c. /etc/login.defs
d. /etc/logrotate.conf

Management decides to implement a risk management system to reduce and maintain the organizationâ€™s risk to an acceptable level. Which of the following is the correct order in the risk management phase?

a. Risk identification, risk assessment, risk treatment, risk monitoring and review
b. Risk treatment, risk monitoring and review, risk identification, risk assessment
c. Risk assessment, risk treatment, risk monitoring and review, risk identification
d. Risk identification, risk assessment, risk monitoring and review, risk treatment

---

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?

a. tcp.flags==000x0
b. tcp.flags==0x000
c. tcp.flags==0000x
d. tcp.flags==x0000

Sam wants to implement a network-based IDS and finalizes an IDS solution that works based on pattern matching. Which type of network-based IDS is Sam implementing?

a. Anomaly-based IDS
b. Behavior-based IDS
c. Stateful protocol analysis
d. Signature-based IDS

Based on which of the following registry key, the Windows Event log audit configurations are recorded?

a. HKEY_LOCAL_MACHINE\SYSTEM\Services\EventLog\ < ErrDev >
b. HKEY_LOCAL_MACHINE\CurrentControlSet\Services\EventLog\< ESENT >
c. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ < Event Log >
d. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ EventLog\ < EntAppsvc >

John, a network administrator, is configuring Amazon EC2 cloud service for his organization. Identify the type of cloud service modules his organization adopted.

a. Platform-as-a-Service (PaaS)
b. Storage-as-a-Service (STaaS)
c. Software-as-a-Service (SaaS)
d. Infrastructure-as-a-Service (IaaS)

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, have to choose?

a. Promiscuous policy
b. Permissive policy
c. Paranoid policy
d. Prudent policy

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?

a. Centrally assign Windows PC group policies
b. Install antivirus software and turn off unnecessary services
c. Dedicate a partition on HDD and format the disk using NTFS
d. Download and install latest patches and enable Windows Automatic Updates

---

Identify the virtualization level that creates a massive pool of storage areas for different virtual machines running on the hardware

a. File system virtualization
b. Fabric virtualization
c. Server virtualization
d. Storage device virtualization

Which of the following things need to be identified during attack surface visualization?

a. Attacker's tools, techniques, and procedures
b. Regulatory frameworks, standards and, procedures for organizations
c. Authentication, authorization, and auditing in networks
d. Assets, topologies, and policies of the organization

Phishing-like attempts that present users a fake usage bill of the cloud provider is an example of a

a. User to cloud attack surface
b. User to service attack surface
c. Cloud to service attack surface
d. Cloud to user attack surface

How is a “risk” represented?

a. Motive (goal) + method + vulnerability
b. Asset + threat + vulnerability
c. Motive (goal) + method
d. Asset + threat

Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

a. Verification
b. Mitigation
c. Remediation
d. Assessment

Identify the attack signature analysis technique carried out when attack signatures are contained in packet headers.

a. Context-based signature analysis
b. Content-based signature analysis
c. Atomic signature-based analysis
d. Composite signature-based analysis

Who is an IR custodian?

a. An individual responsible for conveying company details after an incident
b. An individual who makes a decision on the classifications and the severity of the incident identified
c. An individual who receives the initial IR alerts and leads the IR team in all the IR activities
d. An individual responsible for the remediation and resolution of the incident that occurred

---

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?

a. Research honeypot
b. Low-interaction honeypots
c. Pure honeypots
d. High-interaction honeypots

Which of the following helps in viewing account activity and events for supported services made by AWS?

a. AWS Certificate Manager
b. AWS CloudHSM
c. AWS CloudFormation
d. AWS CloudTrial

John has implemented _____ in the network to restrict the number of public IP addresses in his organization and to enhance the firewall filtering technique.

a. DMZ
b. Proxies
c. NAT
d. VPN

Leslie, the network administrator of Livewire Technologies, has been recommending multilayer inspection firewalls to deploy the companyâ€™s infrastructure. What layers of the TCP/IP model can it protect?

a. Application, TCP, and IP
b. Application, IP, and network interface
c. Network interface, TCP, and IP
d. IP, application, and network interface

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 to calculate the false positive rate?

a. False negative/(true negative+true positive)
b. True negative/(false negative+true positive)
c. False positive/(false positive+true negative)
d. False negative/(false negative+true positive)

Which of the following refers to the data that is stored or processed by RAM, CPUs, or databases?

a. Data at Rest
b. Data in Backup
c. Data is Use
d. Data in Transit

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 organizationâ€™s network. Which of following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt? (Select all that apply.)

a. tcp.options.mss_val<1460
b. tcp.options.wscale_val==20
c. tcp.flags==0x2b
d. tcp.flags=0x00

John wants to implement a packet filtering firewall in his organizationâ€™s network. What TCP/IP layer does a packet filtering firewall work on?

a. Network interface layer
b. IP layer
c. TCP layer
d. Application layer

How is an â€œattackâ€ represented?

a. Asset + Threat
b. Asset + Threat + Vulnerability
c. Motive (goal) + method
d. Motive (goal) + method + vulnerability

What cryptography technique can encrypt small amounts of data and applies it to digital signatures?

a. Hashing
b. Digital certificates
c. Asymmetric encryption
d. Symmetric encryption

Choose the correct order of steps to analyze the attack surface.

a. Visualize the attack surface->simulate the attack->identify the indicators of exposure->reduce the attack surface
b. Visualize the attack surface->identify the indicators of exposure->simulate the attack->reduce the attack surface
c. Identify the indicators of exposure->simulate the attack->visualize the attack surface->reduce the attack surface
d. Identify the indicators of exposure->visualize the attack surface->simulate the attack->reduce the attack surface

---

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?

a. RAID level 1
b. RAID level 5
c. RAID level 10
d. RAID level 50

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 actions beforehand to defend against them. Which one of the following security defense techniques should he implement?

a. Preventive security approach
b. Proactive security approach
c. Retrospective security approach
d. Reactive security approach

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?

a. Host
b. Perimeter
c. Physical
d. Policies and procedures

Which of the following helps prevent executing untrusted or untested programs or code from untrusted or unverified third-parties?

a. Application whitelisting
b. Application sandboxing
c. Deployment of WAFs
d. Application blacklisting

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.

a. Key risk indicator
b. Risk matrix
c. Risk levels
d. Risk severity

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?

a. # kill -9 [PID]
b. # update-rc.d -f [service name] remove
c. # service [service name] stop
d. # ps ax | grep [Target Process]

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?

a. SecurityPolicyDsc
b. Sysmon
c. MicroBurst (not sure)
d. POSH-Sysmon

Which among the following filter is used to detect a SYN/FIN attack?

a. tcp.flags==0x001
b. tcp.flags==0x004
c. tcp.flags==0x003
d. tcp.flags==0x002

.. (لا تنساني من دعواتك) ..

.. (pray for me too) ..