Exam : **SY0-601**

Title : CompTIA Security+ Exam

Vendor : CompTIA

Version : V37.35

NO.1 A major clothing company recently lost of large of priority information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technician implementation to present this from happeing again?
(A). Configure DLP solution
(B). Disable peer-topeer sharing
(C). Enable role-based access controls.
(D). Mandsha job rotation.
(E). Implement content filters
Answer: A

NO.2 An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?
(A). Screen locks
(B). Application management
(C). Geofencing
(D). Containerization
Answer: D A

NO.3 An organization has hired a ted team to simulate attacks on its security posture Which of the following will the blue team do after detecting an loC?
(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
Answer: B

NO.4 Which of the following are common VoIP-associated vulnerabilities? (Select TWO).
(A). SPIM
(B). vishing
(C). Hopping
(D). Phishing
(E). Credential harvesting
(F). Tailgating
Answer: A,B BE

NO.5 Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?
(A). Common Weakness Enumeration
(B). OSINT
(C). Dark web
(D). Vulnerability databases
Answer: C

NO.6 An organization would like to give remote workers the ability to use applications hosted inside the corporate network Users will be allowed to use their personal computers or they will be provided

organization assets Either way no data or applications will be installed locally on any user systems Which of the following mobile solutions would accomplish these goals?
(A). VDI
(B). MDM
(C). COPE
(D). UTM
Answer: A
MDM would require something to be installed. VDI, virtual desktop infrastructure, would allow employees to use run apps on the company network without installing locally.

NO.7 When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?
(A). Tokenization
(B). Data masking
(C). Normalization
(D). Obfuscation
Answer: C

NO.8 An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?
(A). Quarantining the compromised accounts and computers, only providing them with network access
(B). Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
(C). Isolating the compromised accounts and computers, cutting off all network and internet access.
(D). Logging off and deleting the compromised accounts and computers to eliminate attacker access.
Answer: B

* **NO.9** A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system Which of the following would be BEST suited for this task?
(A). Social media analysis
(B). Annual information security training
(C). Gamification
(D). Phishing campaign
Answer: C

NO.10 A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?
(A). IP restrictions
(B). Multifactor authentication
(C). A banned password list
(D). A complex password policy

Answer: B

NO.11 A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?
(A). Create an OCSP
(B). Generate a CSR
(C). Create a CRL
(D). Generate a .pfx file
Answer: B
A certificate signing request (CSR) is one of the first steps towards getting your own SSL/TLS certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key. We'll go into more details on the roles of these keys below.

NO.12 A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?
(A). Domain reputation
(B). Domain hijacking
(C). Disassociation
(D). DNS poisoning
Answer: D

NO.13 After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest, Which of the following compliance frameworks would address the compliance team's GREATEST concern?
(A). PCI DSS
(B). GDPR
(C). ISO 27001
(D). NIST CSF
Answer: A

NO.14 A security policy states that common words should not be used as passwords. A security auditor was able to perform a dictionary attack against corporate credentials Which of the following controls was being violated?
(A). Password complexity

(B). Password history
(C). Password reuse
(D). Password length
Answer: B

A

NO.15 Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?
(A). Job rotation policy
(B). NDA
(C). AUP
(D). Separation Of duties policy
Answer: A

C

NO.16 Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?
(A). Recovery
(B). Deterrent
(C). Corrective
(D). Detective
Answer: C
Corrective controls are implemented after detective controls to rectify the problem and (ideally) prevent it from happening again.

NO.17 A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution In order to reslnct PHI documents which of the following should be performed FIRST?
(A). Retention
(B). Governance
(C). Classification
(D). Change management
Answer: C

NO.18 A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)
(A). Perform a site survey
(B). Deploy an FTK Imager
(C). Create a heat map
(D). Scan for rogue access points
(E). Upgrade the security protocols
Answer: A,C

NO.19 A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?
(A). MSSP

(B). SOAR
(C). IaaS
(D). PaaS
Answer: B

NO.20 A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?
(A). DAC
(B). ABAC
(C). SCAP
(D). SOAR
Answer: D

NO.21 The process of passively gathering information prior to launching a cyberattack is called:
(A). tailgating.
(B). reconnaissance.
(C). pharming.
(D). prepending.
Answer: B

NO.22 The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?
(A). The NOC team
(B). The vulnerability management team
(C). The CIRT
(D). The read team
Answer: C

NO.23 An employee received a word processing file that was delivered as an email attachment The subject line and email content enticed the employee to open the attachment. Which of the following attack vectors BEST matches this malware?
(A). Embedded Python code
(B). Macro-enabled file
(C). Bash scripting
(D). Credential-harvesting website
Answer: B

NO.24 Which of the following would be used to find the MOST common web-application vulnerabilities?
(A). OWASP

(B). MITRE ATT&CK
(C). Cyber Kill Chain
(D). SDLC
Answer: A

NO.25 A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?
(A). Configuring signature-based antivirus io update every 30 minutes
(B). Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
(C). Implementing application execution in a sandbox for unknown software.
(D). Fuzzing new files for vulnerabilities if they are not digitally signed
Answer: C

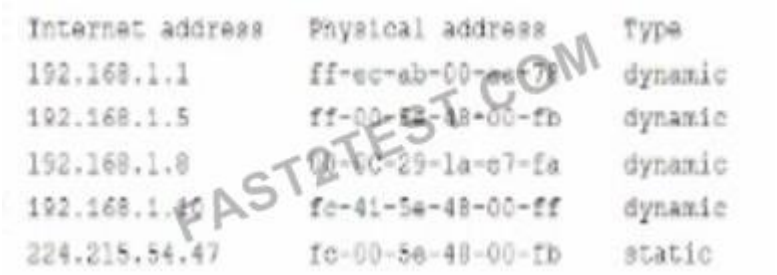
NO.26 A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?
(A). An external access point is engaging in an evil-twin attack.
(B). The signal on the WAP needs to be increased in that section of the building.
(C). The certificates have expired on the devices and need to be reinstalled.
(D). The users in that section of the building are on a VLAN that is being blocked by the firewall
Answer: A

NO.27 A security analyst needs to be able to search and correlate logs from multiple sources in a single tool Which of the following would BEST allow a security analyst to have this ability?
(A). SOAR
(B). SIEM
(C). Log collectors
(D). Network-attached storage
Answer: B
SIEM event correlation is an essential part of any SIEM solution. It aggregates and analyzes log data from across your network applications, systems, and devices, making it possible to discover security threats and malicious patterns of behaviors that otherwise go unnoticed and can lead to compromise or data loss.

NO.28 A secullly operations analyst is using the company's SIEM solufon to correlate alens. Which of the following stages of the Inciden reapanse process is this an example af?
(A). Eradication
(B). Recowery
(C). identiticalion
(D). Preparation

Answer: C

NO.29 A securily analysl has receved several reporls of an issue on an inlemal web application. Users state they are having to provide their credentials brice to log in. The analyst checks with he application team and noles Unis is not an expected bohavier. After looking at several lags, the analysi deciies to in some commands on the gateway and obtains the following output:



Which of the following BEST describes the attack the company is experiencing?
(A). MAC fleoding
(B). URL redirection
(C). ARP paisoning
(D). DNS hijacking
Answer: C

NO.30 An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?
(A). Nmap
(B). cURL
(C). Netcat
(D). Wireshark
Answer: D
https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,packet%20data%20from%20a%20network.

NO.31 In which of the following situations would it be BEST to use a detective control type for mitigation?
(A). A company implemented a network load balancer to ensure 99.999% availability of its web application.
(B). A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
(C). A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
(D). A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
(E). A company purchased liability insurance for flood protection on all capital assets.
Answer: D

NO.32 A large industrial system's smart generator monitors the system status and sends alerts to

third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?
(A). Segmentation
(B). Firewall whitelisting
(C). Containment
(D). isolation
Answer: A

NO.33 A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?
(A). SaaS
(B). IaaS
(C). PaaS
(D). SDN
Answer: A
In order from the least amount of management, to the most amount of management for the company:
SaaS > PaaS > IaaS > On-site
SaaS - Basically everything is managed by the provider
PaaS - The provider manages everything other than applications and data IaaS - The middle-ground o f services. The provider takes on half, while you take on the other half. Provider is responsible for virtualization, networking, servers, and storage. The company is responsible for applications, data, runtime, OS, and middleware.
On-site - There is no service provider. The company is responsible for the whole pie.
https://www.pcmag.com/picks/the-best-database-as-a-service-solutions

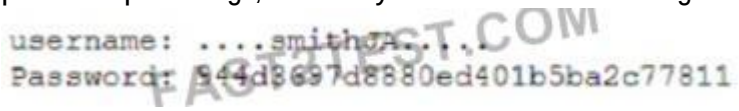
NO.34 A recent phishing campaign resulted in several compromised user accounts. The security incident response team has been tasked with reducing the manual labor of filtering through all the phishing emails as they arrive and blocking the sender's email address, along with other time-consuming mitigation actions. Which of the following can be configured to streamline those tasks?
(A). SOAR playbook
(B). MOM policy
(C). Firewall rules
(D). URL filter
(E). SIEM data collection
Answer: A

NO.35 An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?
(A). CIS benchmarks
(B). GDPR guidance
(C). Regional regulations

(D). ISO 27001 standards
Answer: A
https://www.beyondtrust.com/resources/glossary/systems-hardening

NO.36 The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?
(A). CASB
(B). VPN concentrator
(C). MFA
(D). VPC endpoint
Answer: A

NO.37 Security analysts notice a server login from a user who has been on vacation for two weeks The analysts confirm that the user did not log in to the system while on vacation After reviewing packet capture logs, the analysts notice the following:



Which of the following occurred?
(A). A buffer overflow was exploited to gain unauthorized access
(B). The user's account was compromised, and an attacker changed the login credentials
(C). An attacker used a pass-the-hash attack to gain access
(D). An insider threat with username smithJA logged in to the account
Answer: B

NO.38 Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?
(A). SIEM
(B). CASB
(C). UTM
(D). DLP
Answer: B
Microsoft has a straightforward definition and it includes DLP. "is a security policy enforcement point positioned between enterprise users and cloud service providers" https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb A cloud access security broker (CASB) works by securing data flowing to and from in-house IT architectures and cloud vendor environments using an organization's security policies. CASBs protect enterprise systems against cyberattacks through malware prevention and provide data security through encryption, making data streams unreadable to outside parties. CASBs were created with one thing in mind: protecting proprietary data stored in external, third-party media. CASBs deliver capabilities not generally available in traditional controls such as secure web gateways (SWGs) and enterprise firewalls. CASBs provide policy and governance concurrently across multiple cloud services and provide granular visibility into and control over user activities. https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker

NO.39 A network engineer notices the VPN concentrator overloaded and crashes on days when

there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?
(A). iPSec
(B). Always On
(C). Split tunneling
(D). L2TP
Answer: B

NO.40 An ofgantzation has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk
(A). avoidance
(B). acceptance
(C). mitigation
(D). transference
Answer: D

NO.41 Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function property. Which of the following should the security administrator consider implementing to address this issue?
(A). Application code signing
(B). Application whitellsting
(C). Data loss prevention
(D). Web application firewalls
Answer: B

NO.42 Which of the following is assured when a user signs an email using a private key?
(A). Non-repudiation
(B). Confidentiality
(C). Availably
(D). Authentication
Answer: A
Non Repudiation is your virtual John Hancock. It's a way of virtually stamping any data or document with "I am who I say I am". Only way to break this would be if the private key owners' private key became compromised. Which at that point you got bigger problems than Non Repudiation.

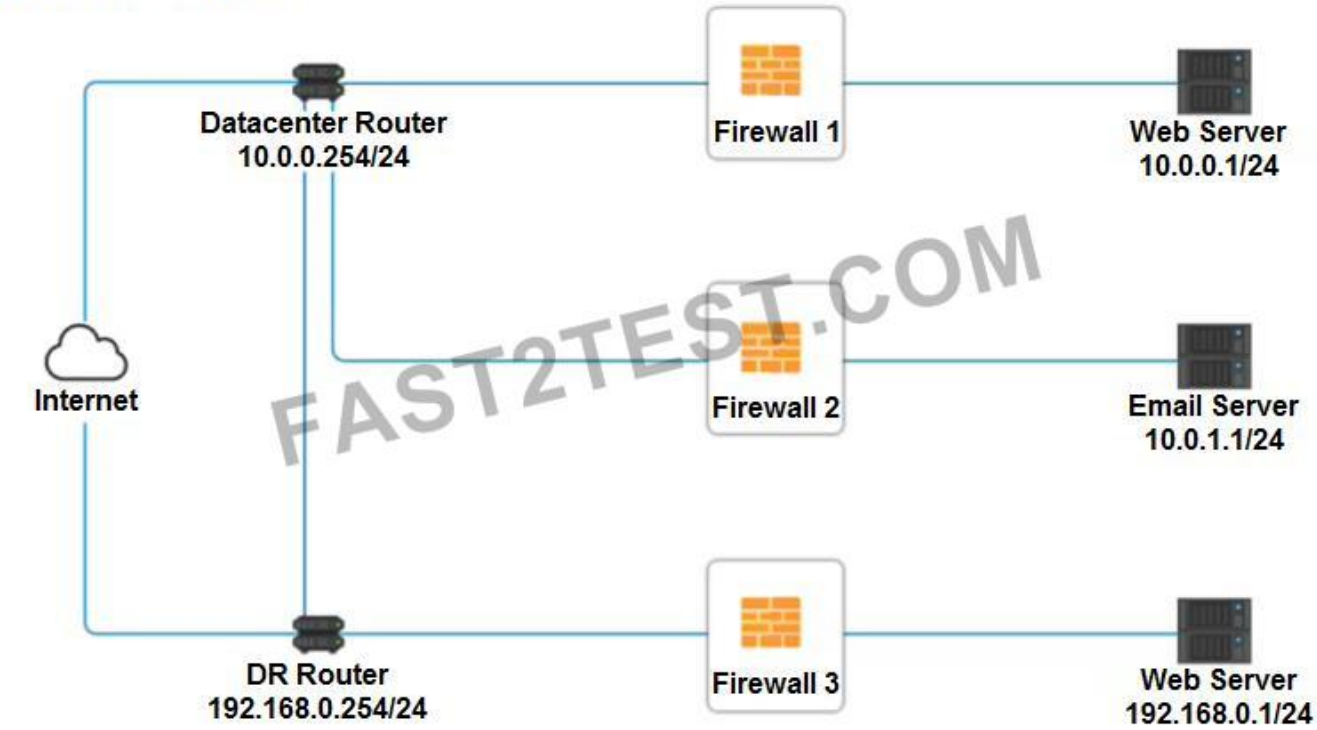
NO.43 Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?
(A). Version control
(B). Continuous monitoring
(C). Stored procedures
(D). Automation
Answer: A

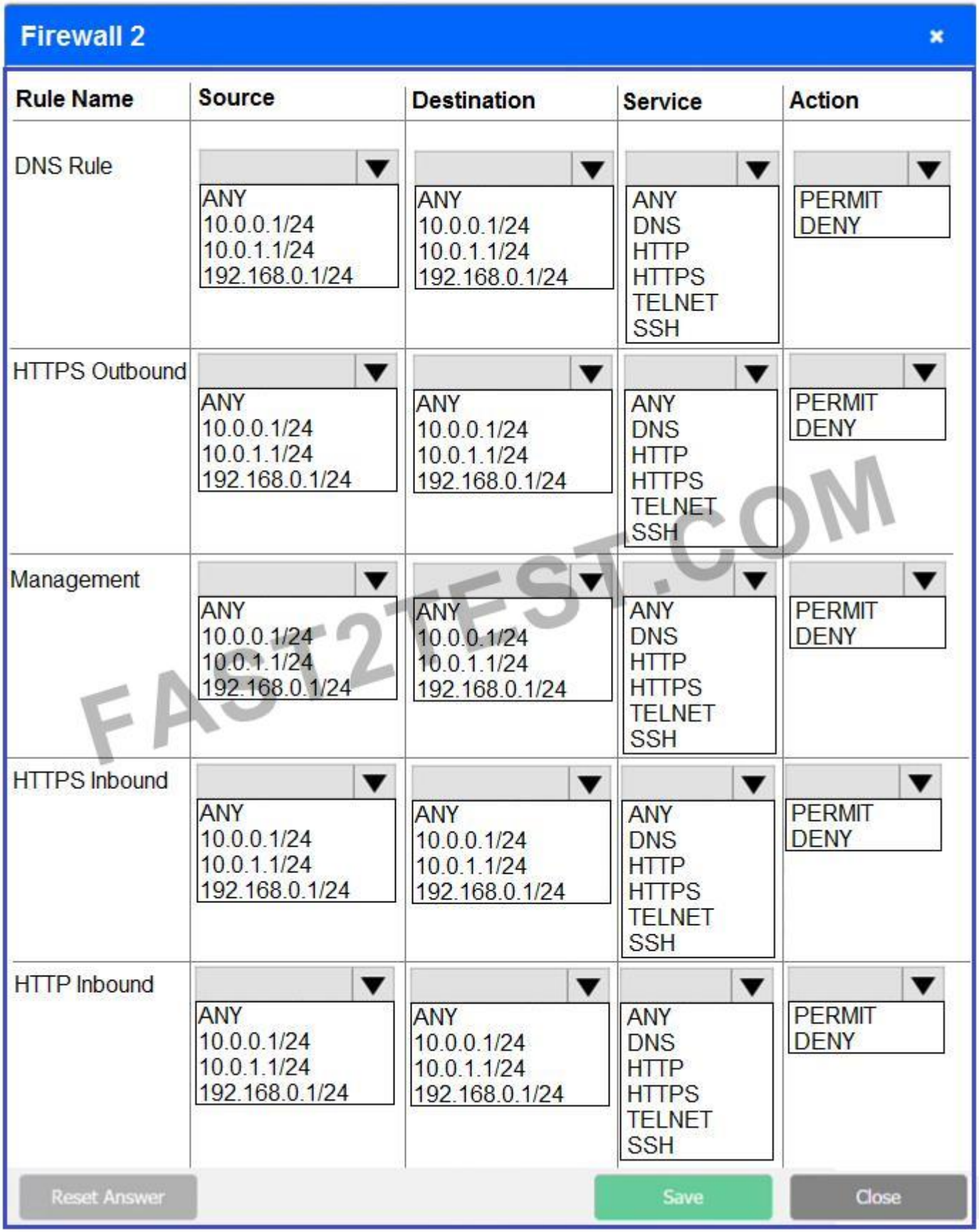
https://www.perforce.com/blog/vcs/what-is-version-control

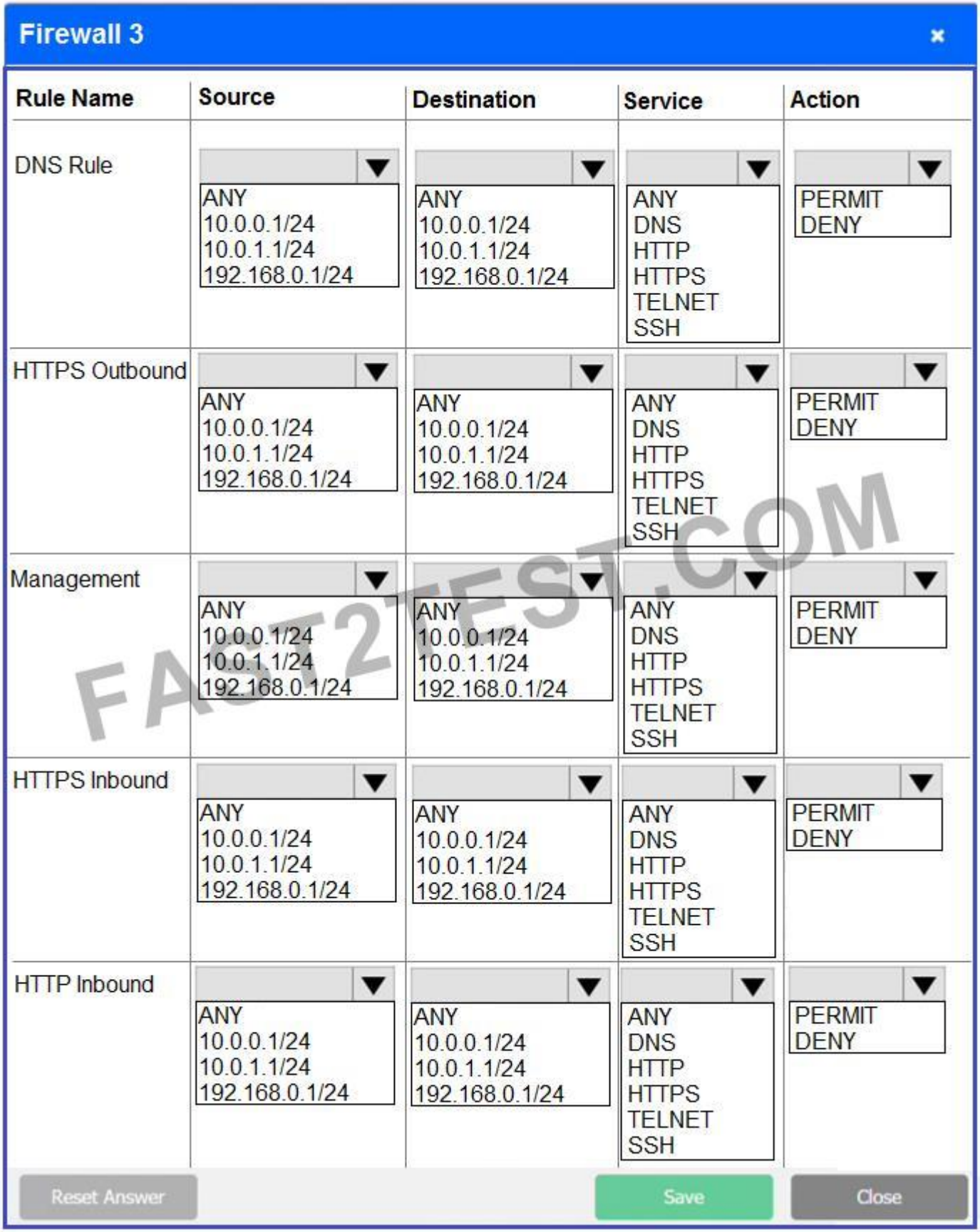
NO.44 A network engineer created two subnets that will be used for production and development servers. Per security policy, production and development servers must each have a dedicated network that cannot communicate with one another directly. Which of the following should be deployed so that server administrators can access these devices?
(A). VLANS
(B). Internet proxy servers
(C). NIDS
(D). Jump servers
Answer: D

NO.45 A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
Deny cleartext web traffic.
Ensure secure management protocols are used. Please Resolve issues at the DR site.
The ruleset order cannot be modified due to outside constraints.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram





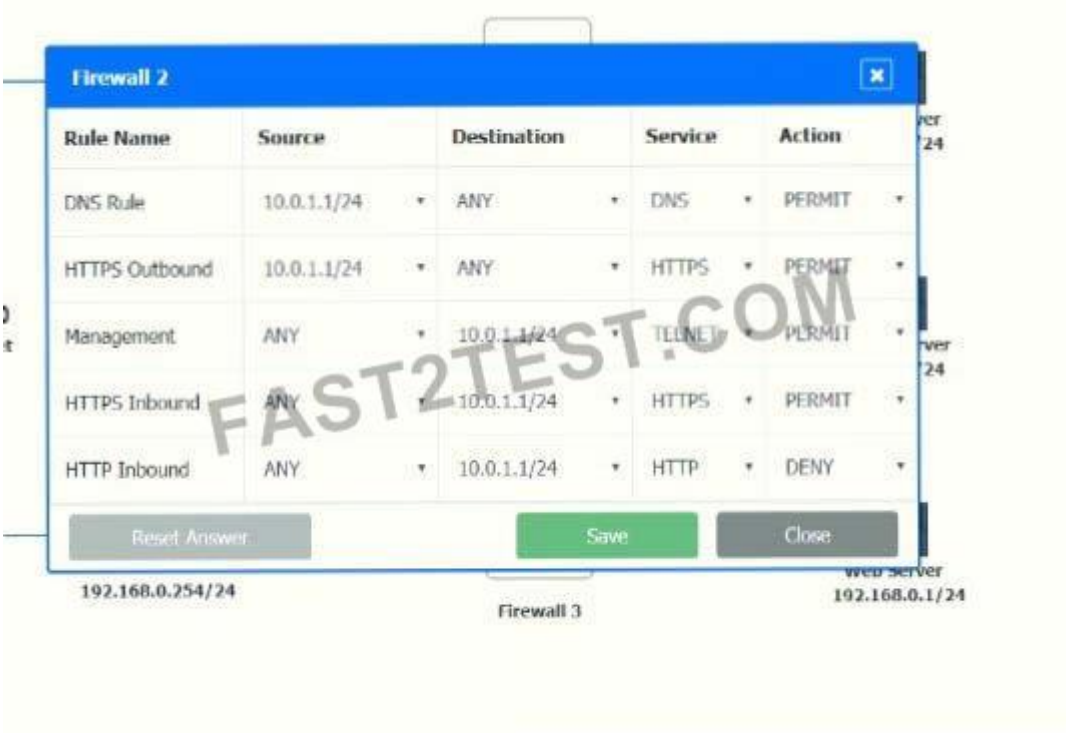


Answer:

Firewall 1:

DNS Rule - ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound - 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY
Firewall 2: No changes should be made to this firewall



Firewall 3:
DNS Rule - ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound - 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY

NO.46 After reluming from a conference, a user's laptop has been operating slower than normal and overheating and the fans have been running constantly Dunng the diagnosis process, an unknown piece of hardware is found connected to the laptop's motherboard Which of the following attack vectors was exploited to install the hardware?
(A). Removable media
(B). Spear phishing
(C). Supply chain
(D). Direct access
Answer: D

NO.47 Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?
(A). DLP
(B). NIDS
(C). TPM
(D). FDE
Answer: A
Data loss prevention (DLP) makes sure that users do not send sensitive or critical information outside the corporate network

NO.48 Two hospitals merged into a single organization. The privacy officer requested a review of all records to ensure encryption was used during record storage, in compliance with regulations. During the review, the officer discovered thai medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?
(A). Personal health information
(B). Personally Identifiable Information
(C). ToKenized data
(D). Proprietary data
Answer: A

NO.49 A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations Every day each location expenences very bnef outages that last for a few seconds However dunng the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an jndustnal smelter. Which of the following is the BEST solution to reduce the risk of data loss?
(A). Dual supply
(B). Generator
(C). PDU
(D). Daily backups
Answer: B C

NO.50 Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?
(A). The business continuity plan

(B). The retention policy
(C). The disaster recovery plan
(D). The incident response plan
Answer: A
BCP is to empower an organization to keep crucial functions running during downtime. This, in turn, helps the organization respond quickly to an interruption, while creating resilient operational protocols.

NO.51 During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?
(A). dd
(B). memdump
(C). tcpdump
(D). head
Answer: A

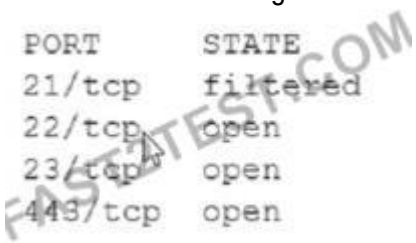
NO.52 Which of the following secure coding techniques makes compromised code more difficult for hackers to use?
(A). Obfuscation
(B). Normalization
(C). Execution
(D). Reuse
Answer: A
https://en.wikipedia.org/wiki/Obfuscation_(software)

NO.53 Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public Which of the following security solutions would mitigate the risk of future data disclosures?
(A). FDE
(B). TPM
(C). HIDS
(D). VPN
Answer: A

NO.54 After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company Which of the following risk management strategies is the manager adopting?
(A). Risk acceptance
(B). Risk avoidance
(C). Risk transference
(D). Risk mitigation
Answer: C

NO.55 A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?
(A). Semi-authorized hackers
(B). State actors
(C). Script kiddies
(D). Advanced persistent threats
Answer: B

NO.56 An analyst Is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap:



Which of the following should the analyst recommend to disable?
(A). 21/tcp
(B). 22/tcp
(C). 23/tcp
(D). 443/tcp
Answer: C

NO.57 Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?
(A). Smart card
(B). push notifications
(C). Attestation service
(D). HMAC-based, one-time password
Answer: B

NO.58 A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?
(A). Monitoring large data transfer transactions in the firewall logs
(B). Developing mandatory training to educate employees about the removable media policy
(C). Implementing a group policy to block user access to system files
(D). Blocking removable-media devices and write capabilities using a host-based security tool
Answer: D

NO.59 Which of the following is a reason why an organization would define an AUP?
(A). To define the lowest level of privileges needed for access and use of the organization's resources
(B). To define the set of rules and behaviors for users of the organization's IT systems
(C). To define the intended partnership between two organizations

(D). To define the availability and reliability characteristics between an IT provider and consumer
Answer: A

B

NO.60 Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?
(A). Unsecured root accounts
(B). Zero day
(C). Shared tenancy
(D). Insider threat
Answer: C

NO.61 Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?
(A). Install a definition-based antivirus.
(B). Implement an IDS/IPS
(C). Implement a heuristic behavior-detection solution.
(D). Implement CASB to protect the network shares.
Answer: C
Heuristic analysis is also one of the few methods capable of combating polymorphic viruses - the term for malicious code that constantly changes and adapts. Heuristic analysis is incorporated into advanced security solutions offered by companies like Kaspersky Labs to detect new threats before they cause harm, without the need for a specific signature. https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis

NO.62 Accompany has a flat network that is deployed in the cloud. Security policy states that all production and development servers must be segmented. Which of the following should be used to design the network to meet the security requirements?
(A). CASB
(B). VPC
(C). Perimeter network
(D). WAF
Answer: A

NO.63 A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?
(A). OAuth
(B). TACACS+
(C). SAML
(D). RADIUS
Answer: D

C

NO.64 A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

(A). openssl
(B). hping
(C). netcat
(D). tcpdump
Answer: A

D

NO.65 A software company adopted the following processes before releasing software to production;
* Peer review
* Static code scanning
* Signing
A considerable number of vulnerabilities are still being detected when code is executed on production Which of the following security tools can improve vulnerability detection on this environment?
(A). File integrity monitonng for the source code
(B). Dynamic code analysis tool
(C). Encrypted code repository
(D). Endpoint detection and response solution
Answer: A

B

NO.66 Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?
(A). The key length of the encryption algorithm
(B). The encryption algorithm's longevity
(C). A method of introducing entropy into key calculations
(D). The computational overhead of calculating the encryption key
Answer: B

NO.67 A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?
(A). CVE
(B). SIEM
(C). SOAR
(D). CVSS
Answer: D
The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability, and is an integral component of many vulnerability scanning tools.

NO.68 An amusement park is implementing a btomelnc system that validates customers' fingerpnnts to ensure they are not sharing tickets The park's owner values customers above all and would prefer customers' convenience over security For this reason which of the following features should the security team prioritize FIRST?
(A). Low FAR
(B). Low efficacy

(C). Low FRR
(D). Low CER
Answer: C
FAR (False Acceptance Rate)
FRR (False Rejection Rate)
CER (Crossover Error Rate) AKA ERR (Equal Error Rate)
since he is willing to sacrifice Security for Customer Service, Best way to understand this is.
FAR has to go up in order for FRR to go down.
typical business practice is in the middle of both which would be near the CER.

NO.69 The Spread of misinformation sorrounding the outbreak of a novel on election day led to eligible voters choosing not take risk of going to the polls.
This is an example of:
(A). Prepending
(B). An inflence campaign
(C). A watering-hole attack
(D). Itimidation
(E). Information elicition
Answer: D

B

NO.70 one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?
(A). Birthday collision on the certificate key
(B). DNS hyacking to reroute traffic
(C). Brute force to the access point
(D). A SSUTLS downgrade

Answer: D

NO.71 An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load Which of the following are the BEST options to accomplish this objective'? (Select TWO)
(A). Load balancing
(B). Incremental backups
(C). UPS
(D). RAID
(E). Dual power supply
(F). NIC teaming
Answer: A,D

NO.72 A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?
(A). An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
(B). An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file
(C). An attacker was able to install malware to the CAasdf234 folder and use it to gam administrator nights and launch Outlook
(D). An attacker was able to phish user credentials successfully from an Outlook user profile
Answer: A

NO.73 A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?
(A). Implement open PSK on the APs
(B). Deploy a WAF
(C). Configure WIPS on the APs
(D). Install a captive portal
Answer: D

NO.74 A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?
(A). Verification

(B). Validation
(C). Normalization
(D). Staging
Answer: A

B

NO.75 Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a secunty analyst for further review The security analyst reviews the following metrics:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?
(A). The ISP is dropping outbound connections
(B). The user of the Sales-PC fell for a phishing attack
(C). Corporate PCs have been turned into a botnet
(D). An on-path attack is taking place between PCs and the router
Answer: D

C

NO.76 To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain Which of the following is being used?
(A). PFS
(B). SPF
(C). DMARC
(D). DNSSEC
Answer: B

D

NO.77 A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```


Which of the following BEST describes this kind of attack?
(A). Directory traversal
(B). SQL injection
(C). API
(D). Request forgery
Answer: D

A

NO.78 Which of the following control types is focused primarily on reducing risk before an incident occurs?
(A). Preventive
(B). Deterrent
(C). Corrective
(D). Detective

Answer: D

A

NO.79 An IT security manager requests a report on company information that is publicly available. The manager's concern is that malicious actors will be able to access the data without engaging in active reconnaissance. Which of the following is the MOST efficient approach to perform the analysis?
(A). Provide a domain parameter to tool.
(B). Check public DNS entries using dnsenum.
(C). Perform a vulnerability scan targeting a public company's IR
(D). Execute nmap using the options: scan all ports and sneaky mode.
Answer: D

A

NO.80 A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?
(A). A malicious USB was introduced by an unsuspecting employee.
(B). The ICS firmware was outdated
(C). A local machine has a RAT installed.
(D). The HVAC was connected to the maintenance vendor.
Answer: A

NO.81 Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?
(A). Hashing
(B). Salting
(C). Integrity
(D). Digital signature
Answer: C

A

NO.82 Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?
(A). Implement proper network access restrictions
(B). Initiate a bug bounty program
(C). Classify the system as shadow IT.
(D). Increase the frequency of vulnerability scans
Answer: A

NO.83 A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfilltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfilltrated credentials?
(A). MFA
(B). Lockout
(C). Time-based logins
(D). Password history

Answer: B

A

NO.84 An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?
(A). Access to the organization's servers could be exposed to other cloud-provider clients
(B). The cloud vendor is a new attack vector within the supply chain
(C). Outsourcing the code development adds risk to the cloud provider
(D). Vendor support will cease when the hosting platforms reach EOL.
Answer: B

NO.85 A security analyst is reviewing application logs to determine the source of a breach and locates the following log:

Which Of the following has been observed?
(A). DLL Injection
(B). API attack
(C). SQLI
(D). XSS
Answer: C

NO.86 In which of the following risk management strategies would cybersecurity insurance be used?
(A). Transference
(B). Avoidance
(C). Acceptance
(D). Mitigation
Answer: A

NO.87 A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers Which of the following is the BEST remediation strategy?
(A). Update the base container image and redeploy the environment
(B). Include the containers in the regular patching schedule for servers
(C). Patch each running container individually and test the application
(D). Update the host in which the containers are running
Answer: C

NO.88 A security analyst is hardening a network infrastructure. The analyst is given the following requirements:
* Preserve the use of public IP addresses assigned to equipment on the core router.
* Enable "in transport" encryption protection to the web server with the strongest ciphers.
Which of the following should the analyst implement to meet these requirements? (Select TWO).
(A). Configure VLANs on the core router.
(B). Configure NAT on the core router.
(C). Configure BGP on the core router.
(D). Enable AES encryption on the web server.
(E). Enable 3DES encryption on the web server.

(F). Enable TLSv2 encryption on the web server.
Answer: A,E

BF

NO.89 A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity modem response team The caller asks the technician to verify the network's internal firewall IP address Which of the following 15 the technician's BEST course of action?
(A). Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller
(B). Ask for the callers name, verify the persons identity in the email directory and provide the requested information over the phone
(C). Write down the phone number of the carter if possible, the name of the person requesting the information hang up. and notify the organization's cybersecurity officer
(D). Request the caller send an email for identity verification and provide the requested information via email to the caller
Answer: D

C

NO.90 A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?
(A). Discretionary
(B). Rule-based
(C). Role-based
(D). Mandatory
Answer: D

NO.91 Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?
(A). The document is a honeyfile and is meant to attract the attention of a cyberintruder.
(B). The document is a backup file if the system needs to be recovered.
(C). The document is a standard file that the OS needs to verify the login credentials.
(D). The document is a keylogger that stores all keystrokes should the account be compromised.
Answer: A

NO.92 A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?
(A). An incident response plan
(B). A communications plan
(C). A business continuity plan
(D). A disaster recovery plan
Answer: D

A

NO.93 While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device.
Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rague system without impacting availability?
(A). Conduct a ping sweep.
(B). Physically check each system.
(C). Deny Internet access to the "UNKNOWN" hostname.
(D). Apply MAC filtering.
Answer: D B

NO.94 A user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?
(A). On-path
(B). Domain hijacking
(C). DNS poisoning
(D). Evil twin
Answer: C B

NO.95 A secutlly analyst needs to perform periodic vulnerabilly scans on produclion ayalems Which of the following scan types would produce the BEST vulnerability scan report?
(A). Port
(B). Intrusive
(C). Host discovery
(D). Credentialed
Answer: D

NO.96 The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:
(A). data controller.
(B). data owner
(C). data custodian.
(D). data processor
Answer: D

NO.97 A company recently experienced a significant data loss when proprietary Information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An Investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the BEST mitigation strategy to prevent

this from happening in the future?
(A). User training
(B). CASB
(C). MDM
(D). EDR
Answer: D

DLP

NO.98 A security analyst Is investigating a malware incident at a company. The malware is accessing a command-and-control website at www.comptia.com. All outbound Intemet traffic is logged to a syslog server and stored in / logfiles/messages. Which of the following commands would be BEST for the analyst to use on the syslog server to search for recent traffic to the command-and-control website?
(A). head -500 www.comptia.com | grep /logfiles/messages
(B). cat /logfiles/messages | tail -500 wew.comptia.com
(C). tail -500 /legfiles/messages | grep www.comptia.com
(D). grep -500 /logfiles/messages | cat www.comptia.com
Answer: B

C

NO.99 Which of the following is the MOST effective control against zero-day vulnerabilities?
(A). Network segmentation
(B). Patch management
(C). Intrusion prevention system
(D). Multiple vulnerability scanners
Answer: A

NO.100 A company wants to simplify the certificate management process. 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). Subject alternative name
(B). Wildcard
(C). Self-signed
(D). Domain validation
Answer: B
Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.' For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.
A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.
https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/

NO.101 Which of the following is a security best practice that ensures the integrity of aggregated log files within a SIEM?

(A). Set up hashing on the source log file servers that complies with local regulatory requirements,
(B). Back up the aggregated log files at least two times a day or as stated by local regulatory requirements.
(C). Write protect the aggregated log files and move them to an isolated server with limited access.
(D). Back up the source log files and archive them for at least six years or in accordance with local regulatory requirements.
Answer: A

NO.102 Which of the following is a reason to publish files' hashes?
(A). To validate the integrity of the files
(B). To verify if the software was digitally signed
(C). To use the hash as a software activation key
(D). To use the hash as a decryption passphrase
Answer: A

NO.103 A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).
(A). Identity processor
(B). Service requestor
(C). Identity provider
(D). Service provider
(E). Tokenized resource
(F). Notarized referral
Answer: B,C

CE

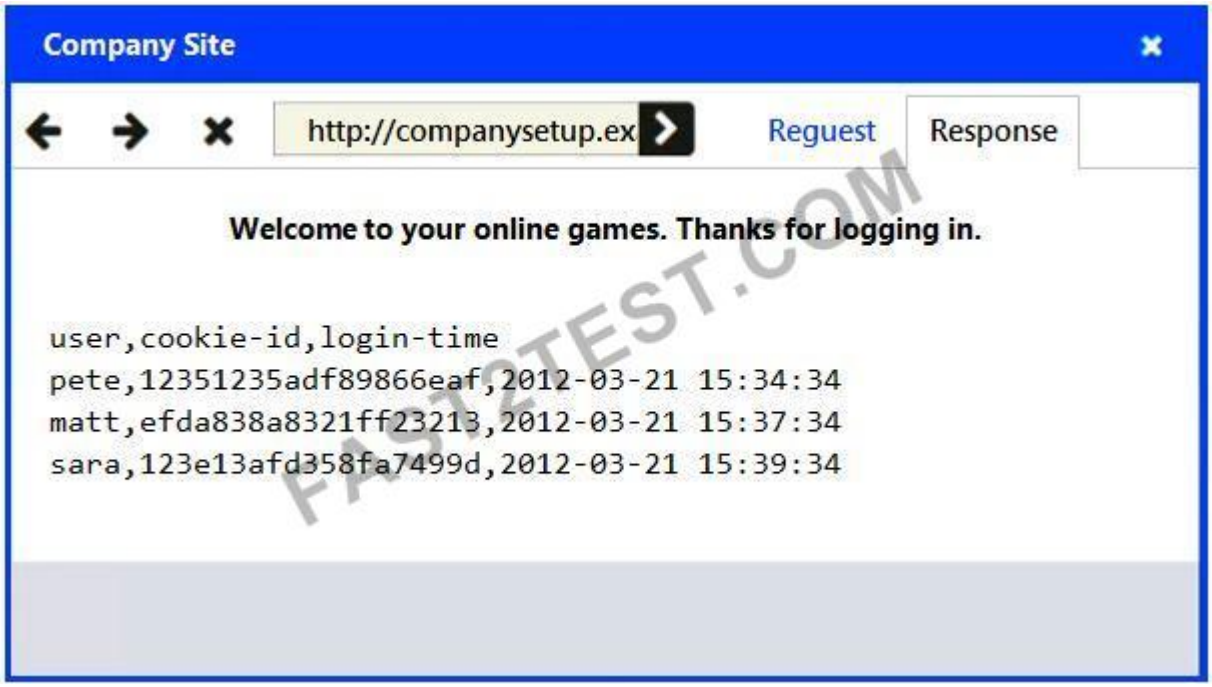
NO.104 In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?
(A). Authority
(B). Intimidation
(C). Consensus
(D). Scarcity
Answer: B

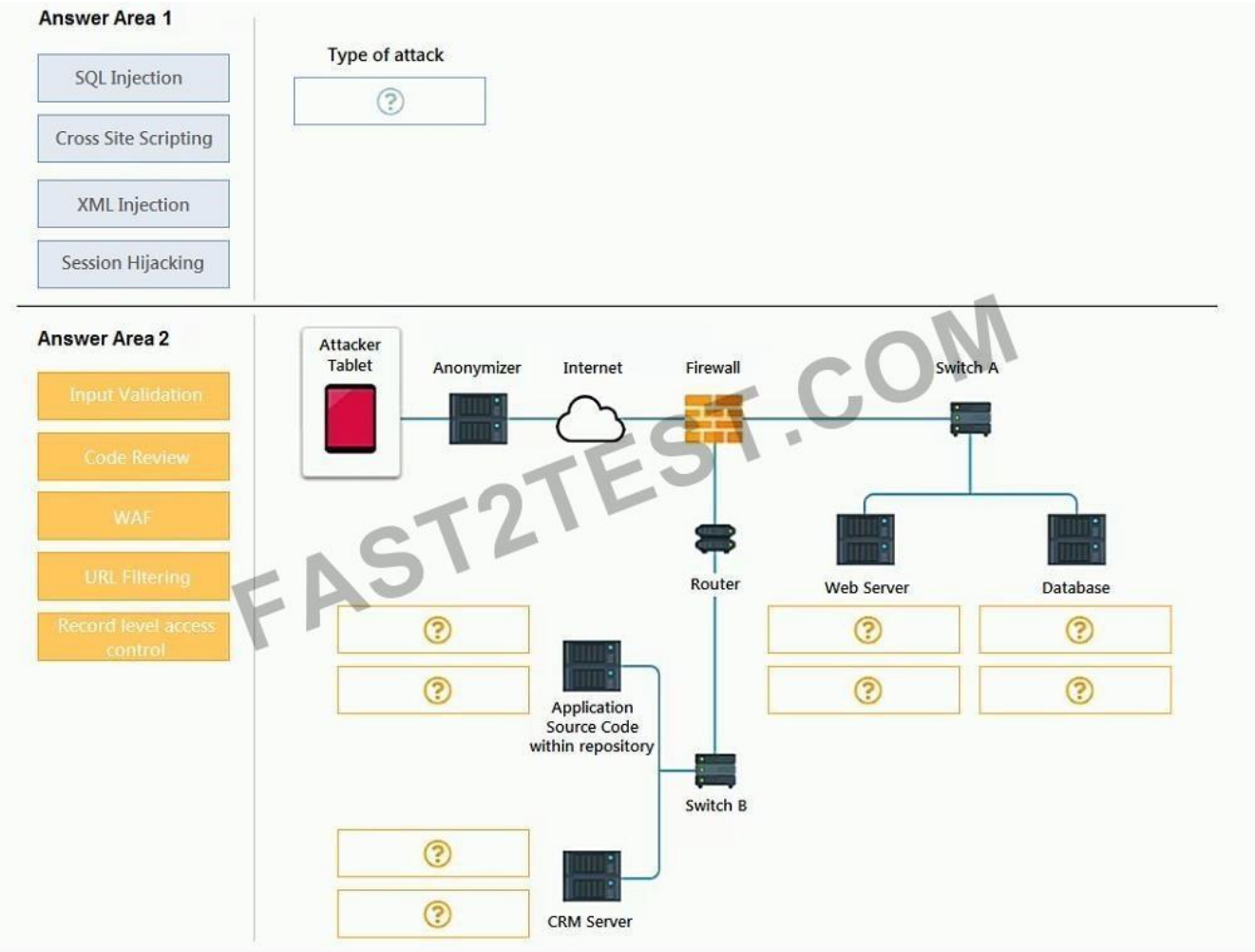
NO.105 An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering it the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?
(A). Disallow new hires from using mobile devices for six months
(B). Select four devices for the sales department to use in a CYOD model
(C). Implement BYOD for the sates department while leveraging the MDM
(D). Deploy mobile devices using the COPE methodology

Answer: C

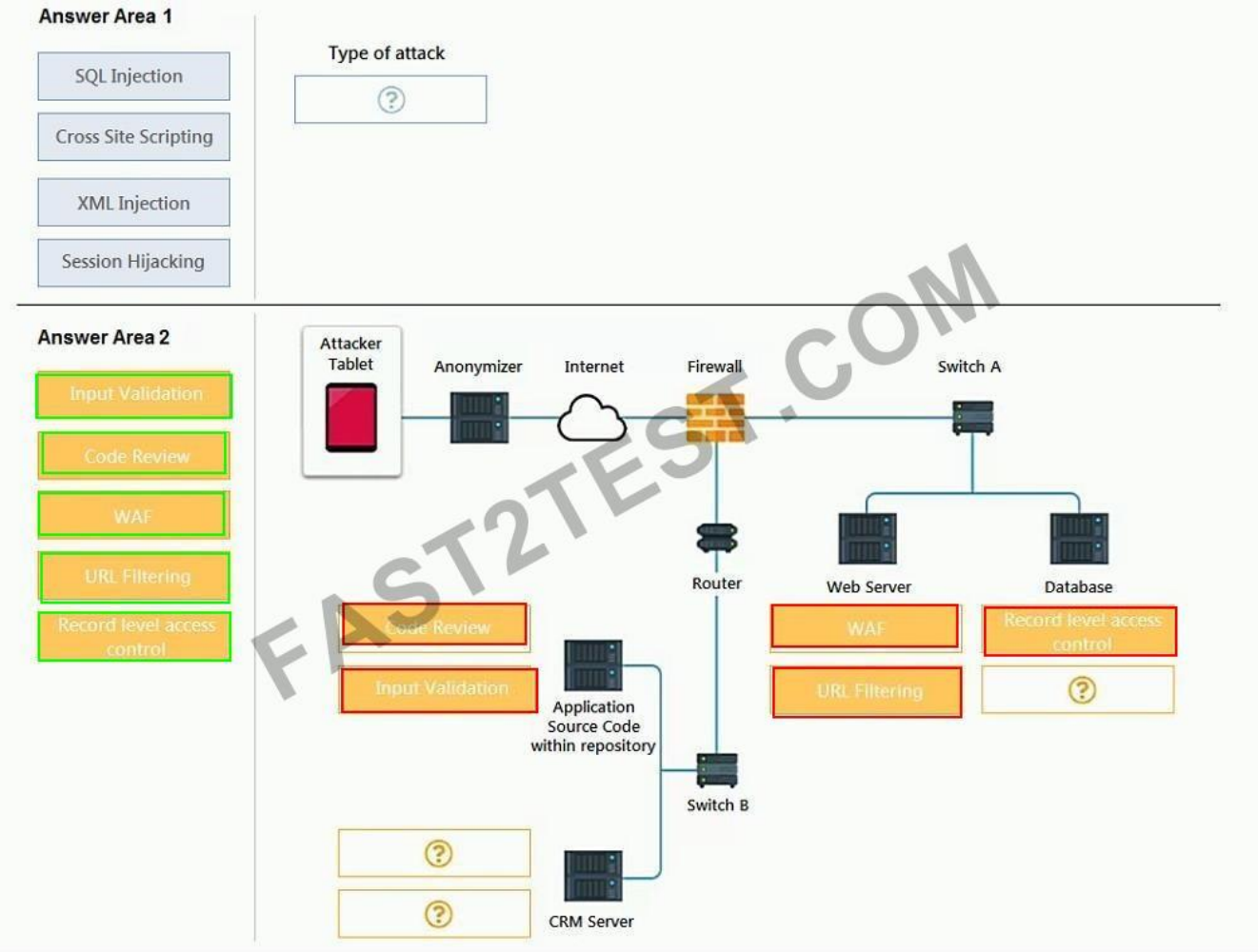
NO.106 A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboars are cleaned and all desks are cleared. The company is MOST likely trying to protect against.
(A). Loss of proprietary information
(B). Damage to the company's reputation
(C). Social engineering
(D). Credential exposure
Answer: C
A

NO.107 An attack has occurred against a company.
INSTRUCTIONS
You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).
Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.
(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.




Answer Area 1
SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking
Type of attack
Answer Area 2
Input Validation
Code Review
WAF
URL Filtering
Record level access control
Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Application Source Code within repository
Switch B
CRM Server
FAST2TEST.COM

Answer:



NO.108 An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).
(A). Iso
(B). PCI DSS
(C). soc
(D). . GDPR
(E). CSA
(F). NIST
Answer: B,D

NO.109 A security researcher has aferted an organuzation that its sensifive user data was found for sale on a website. Which af the followang should the organzabon use to inform the affected partes?
(A). A An incident response plan
(B). A communications plan
(C). A business continuity plan
(D). A disaster recovery plan
Answer: A

NO.110 An analyst is working onan email incident in which target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?
(A). Apply a DLP solution
(B). Implement network segmentation.
(C). Utilize email content filtering.
(D). Isolate the infected attachment.
Answer: B

NO.111 Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?
(A). Development
(B). Staging
(C). Production
(D). Test
Answer: B A

NO.112 Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?
(A). MOU
(B). MTTR
(C). SLA
(D). NDA
Answer: C

NO.113 Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities After further investigation, a security analyst notices the following
* All users share workstations throughout the day
* Endpoint protection was disabled on several workstations throughout the network.
* Travel times on logins from the affected users are impossible
* Sensitive data is being uploaded to external sites
* All usee account passwords were forced lo be reset and the issue continued Which of the following attacks is being used to compromise the user accounts?
(A). Brute-force
(B). Keylogger
(C). Dictionary
(D). Rainbow
Answer: C B

NO.114 Several universities are participating m a collaborative research project and need to share compute and storage resources Which of the following cloud deployment strategies would BEST meet this need?
(A). Community
(B). Private
(C). Public

(D). Hybrid

Answer: A

Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

NO.115 An administrator is experiencing issues when trying to upload a support file to a vendor A pop-up message reveals that a payment card number was found in the file, and the file upload was Mocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

(A). DLP

(B). Firewall rule

(C). Content filter

(D). MDM

(E). Application allow list

Answer: A

NO.116 A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?

(A). Port

(B). Intrusive

(C). Host discovery

(D). Credentialed

Answer: D

NO.117 A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

(A). Perform e@ vulnerability scan to identify the weak spots.

(B). Use a packet analyzer to investigate the NetFlow traffic

(C). Check the SIEM to review the correlated logs.

(D). Require access to the routers to view current sessions,

Answer: C

NO.118 Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

(A). Shut down the VDI and copy off the event logs.

(B). Take a memory snapshot of the running system.

(C). Use NetFlow to identify command-and-control IPs.

(D). Run a full on-demand scan of the root volume.

Answer: B

NO.119 An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?
(A). NGFW
(B). Pagefile
(C). NetFlow
(D). RAM
Answer: C

B

NO.120 A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?
(A). inability to authenticate
(B). Implied trust
(C). Lack of computing power
(D). Unavailable patch

Answer: D

NO.121 A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company.
information on user devices. Which of the following solutions would BEST support the policy?
(A). Mobile device management
(B). Full-device encryption
(C). Remote wipe
(D). Biometrics
Answer: A

NO.122 A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is MOST likely the cause?
(A). The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
(B). The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
(C). The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
(D). The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.
Answer: D

NO.123 A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?
(A). RA1D 0

(B). RAID1
(C). RAID 5
(D). RAID 10
Answer: A
https://techgenix.com/raid-10-vs-raid-5/

D

NO.124 An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?
(A). FRR
(B). Difficulty of use
(C). Cost
(D). FAR
(E). CER
Answer: A

E

NO.125 During a recent security assessment, a vulnerability was found in a common OS, The OS vendor was unaware of the issue and promised to release a patch within next quarter, Which of the following BEST describes this type of vulnerability?
(A). Legacy operating system
(B). Weak configuration
(C). Zero day
(D). Supply chain
Answer: C

A

NO.126 A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?
(A). HTTP security header
(B). DNSSEC implementation
(C). SRTP
(D). S/MIME
Answer: C

A

NO.127 A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.
The task list shows the following results

Name	CPU %	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?
(A). RAT

(B). PUP
(C). Spyware
(D). Keylogger
Answer: A

NO.128 A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?
(A). A RAT
(B). Ransomware
(C). Polymophic
(D). A worm
Answer: C

NO.129 A security analyst is reviewing the following command-line output:

```
Internet address      Physical address      Type
192.168.1.1           aa-bb-cc-00-11-22     dynamic
192.168.1.2           aa-bb-cc-00-11-22     dynamic
192.168.1.3           aa-bb-cc-00-11-22     dynamic
192.160.1.4           aa-bb-cc-00-11-22     dynamic
192.168.1.5           aa-bb-cc-00-11-22     dynamic
---output omitted---
192.168.1.251         aa-bb-cc-00-11-22     dynamic
192.160.1.252         aa-bb-cc-00-11-22     dynamic
192.168.1.253         aa-bb-cc-00-11-22     dynamic
192.168.1.254         aa-bb-cc-00-11-22     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
```


Which of the following Is the analyst observing?
(A). IGMP spoofing
(B). URL redirection
(C). MAG address cloning
(D). DNS poisoning
Answer: C

NO.130 Which of the following BEST describes when an organization utilizes a ready-to-use application from a cloud provider?
(A). laaS
(B). SaaS
(C). Paas
(D). XaaS
Answer: B
SaaS, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software.

https://www.ibm.com/cloud/learn/iaas-paas-saas

NO.131 After a phishing scam for 9 user's credentals, the red team was able to craft a payload to deploy on @ server. The attack allowed the installaton of malicious software that intiates @ new remote session.
Which of the following types of attacks has occurred?
(A). Privilege escalation
(B). Session replay
(C). Application programming interface
(D). Directory traversal
Answer: A
B

NO.132 A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field. Which of the following concepts does this message describe?
(A). Password complexity
(B). Password reuse
(C). Password history
(D). Password age
Answer: A

NO.133 An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?
(A). SLA
(B). BPA
(C). NDA
(D). MOU
Answer: A

NO.134 The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?
(A). DLP
(B). USB data blocker
(C). USB OTG
(D). Disabling USB ports
Answer: A
B
USB data blockers are good, but they're reliant on the employee actually using them. A DLP solution such as MobileIron forces compliance, by locking corporate resources behind a secure application. For example: Users any mobile device policy, such as BYOD, CYOD, and COPE. If they want to access their corporate email on their phone. They will need to sign into the MobileIron application, in order to be granted visibility to their corporate email account. Since the emails are being read/sent through the MobileIron application. Safeguards can be applied even on an outside network-mobile level. If an employee attempts to send a customers social security number, the MobileIron will either block it,

alert it, or both, contingent on how the company setup the MobileIron service to work.

NO.135 Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?
(A). Production
(B). Test
(C). Staging
(D). Development
Answer: B

NO.136 An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

A.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Deny: Any Any 21
Deny: Any Any
```

B.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Deny: Any Any 22
Allow: Any Any 21
Deny: Any Any
```

C.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 22
Deny: Any Any 67
Deny: Any Any 68
Deny: Any Any 21
Allow: Any Any
```

D.
```
[Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Deny: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Allow: Any Any 21
Allow: Any Any
```


(A). Option A

(B). Option B
(C). Option C
(D). Option D
Answer: A

NO.137 Which of the following actions would be recommended to improve an incident response process?
(A). Train the team to identify the difference between events and incidents
(B). Modify access so the IT team has full access to the compromised assets
(C). Contact the authorities if a cybercrime is suspected
(D). Restrict communication surrounding the response to the IT team
Answer: A

B

NO.138 Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?
(A). An ARO
(B). An MOU
(C). An SLA
(D). A BPA
Answer: B

C

NO.139 Rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?
(A). Configure the perimeter firewall to deny inbound external connections to SMB ports.
(B). Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
(C). Deny unauthenticated users access to shared network folders.
(D). Verify computers are set to install monthly operating system, updates automatically
Answer: A

NO.140 A security analyst must detenmine If elther SSH er Telnet ts being used to lng in bo servers. Which of the following should the analyst use?
(A). legger
(B). Metarup) ost
(C). tepdump
(D). netetat
Answer: D

NO.141 A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?
* The solution must be inline in the network
* The solution must be able to block known malicious traffic
* The solution must be able to stop network-based attacks
Which of the following should the network administrator implement to BEST meet these requirements?
(A). HIDS

(B). NIDS
(C). HIPS
(D). NIPS
Answer: D

NO.142 During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?
(A). 1s
(B). chflags
(C). chmod
(D). lsof
(E). setuid
Answer: C

NO.143 During a Chiet Information Securty Officer (CISO) comvenbon to discuss security awareness, the affendees are provided with a network connection to use as a resource. As the Convention progresses. ane of the attendees starts to notice delays in the connection. and the HTTPS ste requests are reverting to HTTP. Which of the folowing BEST describes what is happening?
(A). Birtuday colfisices on the cartificate key
(B). DNS hijackeng to reroute tratic
(C). Brute force 1 tho access point
(D). A SSL/TLS downgrade
Answer: D

NO.144 A user recently attended an exposition and received some digital promotional materials The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open Which of the following is MOST likely the cause of the reported issue?
(A). There was a drive-by download of malware
(B). The user installed a cryptominer
(C). The OS was corrupted
(D). There was malicious code on the USB drive
Answer: D

NO.145 A security administrator checks the table of a network switch, which shows the following output:

Which of the following is happening to this switch?
(A). MAC Flooding
(B). DNS poisoning
(C). MAC cloning
(D). ARP poisoning
Answer: A

NO.146 A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers.
Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:
(A). perform attribution to specific APTs and nation-state actors.
(B). anonymize any PII that is observed within the IoC data.
(C). add metadata to track the utilization of threat intelligence reports.
(D). assist companies with impact assessments based on the observed data
Answer: B

NO.147 Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?
(A). OWASP
(B). Vulnerability scan results
(C). NIST CSF
(D). Third-party libraries
Answer: A

NO.148 The Chief Information Secunty Officer (CISO) requested a report on potential areas of improvement following a security incident. Which of the following incident response processes is the CISO requesting?
(A). Lessons learned
(B). Preparation
(C). Detection
(D). Containment
(E). Root cause analysis
Answer: A

NO.149 A SOC is implementing an insider-threat-detection program. The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?
(A). honeyfile
(B). ADMZ
(C). DLP
(D). File integrity monitoring
Answer: A

NO.150 A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents Which of the following backup types should be used?
(A). Snapshot
(B). Differential
(C). Cloud
(D). Full
(E). Incremental
Answer: A

NO.151 Which of the following types of controls is a turnstile?
(A). Physical
(B). Detective
(C). Corrective
(D). Technical
Answer: A
https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20(also%20called%20a,%2C%20a%20pass%2C%20or%20similar.

NO.152 Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?
(A). Red team
(B). While team
(C). Blue team
(D). Purple team
Answer: A
Red team-performs the offensive role to try to infiltrate the target.

NO.153 An attacker is attempting to harvest user credentials on a client's wedsite, A security analyst notices multiple attempts of rencom usemames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:
The username you entered does not exist.
Which of the following should the analyst recommend be enabled?
(A). Input validation
(B). Obfuscation
(C). Error handling
(D). Username lockout

Answer: B

C

NO.154 An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?
(A). The theft of portable electronic devices
(B). Geotagging in the metadata of images
(C). Bluesnarfing of mobile devices
(D). Data exfiltration over a mobile hot-spot
Answer: D

NO.155 The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve This type of incident has become more common in recent weeks and is consuming large amounts of the analysts' time due to manual tasks being performed Which of the following solutions should the SOC consider to BEST improve its response time?
(A). Configure a NIDS appliance using a Switched Port Analyzer
(B). Collect OSINT and catalog the artifacts in a central repository
(C). Implement a SOAR with customizable playbooks
(D). Install a SIEM with community-driven threat intelligence
Answer: C
SOAR (Security Orchestration, Automation, and Response) Can use either playbook or runbook. It assists in collecting threat related data from a range of sources and automate responses to low level threats. (frees up some of the CSIRT time)

NO.156 The board of doctors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does the BEST describe?
(A). Transference
(B). Avoidance
(C). Mitigation
(D). Acknowledgement
Answer: A

NO.157 Which of the following is the MOST relevant security check to be performed before embedding third-parry libraries in developed code?
(A). Check to see if the third party has resources to create dedicated development and staging environments.
(B). Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
(C). Assess existing vulnerabilities affecting the third-parry code and the remediation efficiency of the libraries' developers.
(D). Read multiple penetration-testing reports for environments running software that reused the library.
Answer: D

C

NO.158 A large enterprise has moved all Hs data to the cloud behind strong authentication and encryption A sales director recently had a laptop stolen and later, enterprise data was round to have

been compromised database.
Which of the following was the MOST likely cause?
(A). Shadow IT
(B). Credential stuffing
(C). SQL injection
(D). Man-in-the-browser
(E). Bluejacking
Answer: A

NO.159 A security analyst has been tasked with finding the maximum amount of data loss that can occur before ongoing business operations would be impacted. Which of the following terms BEST defines this metric?
(A). MTTR
(B). RTO
(C). RPO
(D). MTBF
Answer: A

NO.160 A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?
(A). RAID 0+1
(B). RAID 2
(C). RAID 5
(D). RAID 6
Answer: C

D

NO.161 An organization is repairing the damage after an incident, Which of the following controls es being implemented?
(A). Detective
(B). Preventive
(C). Corrective
(D). Compensating
Answer: C

NO.162 Administrators have allowed employees to access their company email from personal computers. However, the administrators are concerned that these computers are another attack Surface and can result in user accounts being breached by foreign actors. Which of the following actions would provide the MOST secure solution?
(A). Enable an option in the administration center so accounts can be locked if they are accessed from different geographical areas.
(B). Implement a 16-character minimum length and 30-day expiration password policy.
(C). Set up a global mail rule to disallow the forwarding of any company email to email addresses outside the organization,
(D). Enforce a policy that allows employees to be able to access their email only while they are connected to the Internet via VPN.

Answer: A

D

NO.163 A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?
(A). Outdated software
(B). Weak credentials
(C). Lack of encryption
(D). Backdoors
Answer: B

NO.164 Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.
Which of the following documents did Ann receive?
(A). An annual privacy notice
(B). A non-disclosure agreement
(C). A privileged-user agreement
(D). A memorandum of understanding
Answer: A

NO.165 A symmetric encryption algorithm Is BEST suited for:
(A). key-exchange scalability.
(B). protecting large amounts of data.
(C). providing hashing capabilities,
(D). implementing non-repudiation.
Answer: D

B

NO.166 Whiten of the folowing BEST describes the MFA atiribute tha requires6 calback on a predefined landline?
(A). Something you exchibl
(B). Something you can do
(C). Someone you krcear
(D). Somnewehere pou are
Answer: D

NO.167 After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?
(A). The public ledger
(B). The NetFlow data
(C). A checksum
(D). The event log
Answer: A
https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/

NO.168 The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST

meets the requirements?
(A). SAML
(B). TACACS+
(C). Password vaults
(D). OAuth
Answer: B

NO.169 A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?
(A). Snapshot
(B). Differential
(C). Full
(D). Tape
Answer: B

NO.170 An enterprise has hired an outside security firm to conduct penetration testing on its network and applications.
The firm has only been given the documentation available to the customers of the applications.
Which of the following BEST represents the type of testing that will occur?
(A). Bug bounty
(B). Black-box
(C). Gray-box
(D). White-box
Answer: A

D

NO.171 Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?
(A). Acceptance
(B). Transference
(C). Avoidance
(D). Mitigation
Answer: A

NO.172 Which of the following is a risk that is specifically associated with hosting applications in the public cloud?
(A). Unsecured root accounts
(B). Zero-day
(C). Shared tenancy
(D). Insider threat
Answer: C

NO.173 Which of the following must be in place before implementing a BCP?
(A). SLA
(B). AUP

(C). NDA
(D). BIA
Answer: D

NO.174 A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?
(A). Disable Telnet and force SSH.
(B). Establish a continuous ping.
(C). Utilize an agentless monitor
(D). Enable SNMPv3 With passwords.
Answer: A

NO.175 Atocompany wants to modify its current backup strategy to modity its current backup strategy to minenize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy
(A). Incremental backups followed by differential backups
(B). Full backups followed by incremental backups
(C). Delta backups followed by differental backups
(D). Incremental backups followed by delta backups
(E). Full backup followed by different backups
Answer: A E

NO.176 A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:
(A). employees of other companies and the press
(B). all members of the department that created the documents
(C). only the company's employees and those listed in the document
(D). only the individuate listed in the documents
Answer: A

NO.177 A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files and can work in conjunction with proxies or UTM. Which of the following would BEST meet the CSO's requirements?
(A). Fuzzing
(B). Sandboxing
(C). Static code analysis
(D). Code review
Answer: B

NO.178 ir security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted file"sThe analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?
(A). HIDS
(B). Allow list

(C). TPM
(D). NGFW
Answer: C

D

NO.179 A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?
(A). Dictionary
(B). Rainbow table
(C). Spraying
(D). Brute-force
Answer: D

NO.180 A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).
(A). VPN
(B). Drive encryption
(C). Network firewall
(D). File level encryption
(E). USB blocker
(F). MFA
Answer: B,E

NO.181 A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:
* Must be able to differentiate between users connected to WiFi
* The encryption keys need to change routinely without interrupting the users or forcing reauthentication
* Must be able to integrate with RADIUS
* Must not have any open SSIDs
Which of the following options BEST accommodates these requirements?
(A). WPA2-Enterprise
(B). WPA3-PSK
(C). 802.11n
(D). WPS
Answer: A

C

NO.182 A recent security assessment revealed that an actor explolied a vuinerable workstation willvin an organization and has persisted on the network for several months. The organization realizes the need to reassess Its seourlty strategy for mitigating risks within the perimeter Which of the following solutions woukl BEST support the organization's strategy?
(A). FIM
(B). OOP
(C). EOR
(D). DUT

Answer: C

NO.183 A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)
(A). Trusted Platform Module
(B). A host-based firewall
(C). A DLP solution
(D). Full disk encryption
A VPN
(E). Antivirus software
Answer: A,B

NO.184 An organization maintains several environments in which patches are developed and tested before deployed to an operation status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?
(A). Development
(B). Test
(C). Production
(D). Staging
Answer: D
The staging environment is an optional environment, but it is commonly used when an organization has multiple production environments. After passing testing, the system moves into staging, from where it can be deployed to the different production systems.

NO.185 An organization is developing an authentication service for use at the entry and exit ports of country borders.
The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)
(A). Voice
(B). Gait
(C). Vein
(D). Facial
(E). Retina
(F). Fingerprint
Answer: B,D

NO.186 A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investiga-tion, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discov-ers a couple of WAPs are using the same SSID, but they have non-

standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?
(A). Evil twin
(B). Jamming
(C). DNS poisoning
(D). Bluesnarfing
(E). DDoS
Answer: A

NO.187 Which of the following often operates in a client-server architecture to act as a service repository. provicing enterprise consumers access to structured threat intelligence data?
(A). STIX
(B). CIRT
(C). OSINT
(D). TAXII
Answer: B

A

NO.188 Which of the following in the incident response process is the BEST approach to improve the speed of the identification phase?
(A). Activate verbose logging in all critical assets.
(B). Tune monitoring in order to reduce false positive rates.
(C). Redirect all events to multiple syslog servers.
(D). Increase the number of sensors present on the environment.
Answer: B

NO.189 hich of the following is the BEST method for ensuring non-repudiation?
(A). SSO
(B). Digital certificate
(C). Token
(D). SSH key
Answer: B

NO.190 Which of the following BEST describes a security exploit for which a vendor patch is not readily available?
(A). Integer overflow
(B). Zero-day
(C). End of life
(D). Race condition
Answer: B

NO.191 The process of passively gathering information poor to launching a cyberattack is called:
(A). tailgating
(B). reconnaissance
(C). pharming
(D). prepending
Answer: B

NO.192 Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?
(A). Tabletop
(B). Parallel
(C). Full interruption
(D). Simulation
Answer: D

A

NO.193 A Chief Information Security Officer wants to ensure the organization is validating and checking the Integrity of zone transfers. Which of the following solutions should be implemented?
(A). DNSSEC
(B). LOAPS
(C). NGFW
(D). DLP
Answer: D

A

NO.194 Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?
(A). ISO 27701
(B). The Center for Internet Security
(C). SSAE SOC 2
(D). NIST Risk Management Framework
Answer: B

D

NO.195 An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?
(A). SED
(B). HSM
(C). DLP
(D). TPM
Answer: A

NO.196 Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?
(A). Intelligence fusion
(B). Review reports
(C). Log reviews
(D). Threat feeds
Answer: A

NO.197 An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

(A). MAC filtering
(B). Zero trust segmentation
(C). Network access control
(D). Access control vestibules
(E). Guards
(F). Bollards
Answer: B,D

NO.198 An organization is repairing the damage after an incident, Which of the following controls es being implemented?
(A). Corrective
(B). Compensating
(C). Detective
(D). Preventive
Answer: A

NO.199 While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method. Which of the following would BEST detect a malicious actor?
(A). Utilizing SIEM correlation engines
(B). Deploying Netflow at the network border
(C). Disabling session tokens for all sites
(D). Deploying a WAF for the web server
Answer: A
The initial compromise was a malicious request on a web server. Moments later the token created with SSO was used on another service, the question does not specify what type of service. Deploying a WAF on the web server will detect the attacker but only on that server. If the attacker issues the same malicious request to get another SSO token correlating that event with using that SSO token in other services would allows to detect the malicious activity.

NO.200 A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.
Which of the following tools can the analyst use to verify the permissions?
(A). ssh
(B). chmod
(C). 1s
(D). setuid
(E). nessus
(F). ne

Answer: B

NO.201 A security engineer is installing a WEAF io protect the company's website from malicious wed requests over SSL, Which of the following is needed io meet the objective?
(A). A ere proxy
(B). A Geeryption certificate
(C). A gpill-tunnel VPN

(D). Load-balanced servere
Answer: B

NO.202 A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?
(A). An incident response plan
(B). A communications plan
(C). A disaster recovery plan
(D). A business continuity plan
Answer: D
Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident",[1] and business continuity planning [2][3] (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company.[4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.[5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

NO.203 An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?
(A). The vulnerability scan output
(B). The security logs
(C). The baseline report
(D). The correlation of events
Answer: A

NO.204 As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?
(A). TAXII
(B). TLP
(C). TTP
(D). STIX
Answer: C

NO.205 A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?
(A). The S/MME plug-in is not enabled.
(B). The SLL certificate has expired.
(C). Secure IMAP was not implemented
(D). POP3S is not supported
Answer: A

NO.206 A cyber-security administrator is using an enterprise firewall. The administrator created some rules, but now Seems to be unresponsive. All connections being dropped by the firewall. Which of the following would be the BEST option to remove the rules?
(A). # iptables -t mangle -x
(B). # iptables -f
(C). # iptables -z
(D). # iptables -p input -j drop
Answer: A

NO.207 A user must introduce a password and a USB key to authenticate against a secure computer, and authentication is limited to the state in which the company resides. Which of the following authentication concepts are in use?
(A). Something you know, something you have, and somewhere you are
(B). Something you know, something you can do, and somewhere you are
(C). Something you are, something you know, and something you can exhibit
(D). Something you have, somewhere you are, and someone you know
Answer: A

NO.208 Ann. a forensic analyst. needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?
(A). Chain of custody
(B). Checksums
(C). Non-repudiaton
(D). Legal hold
Answer: A

NO.209 Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the real data?
(A). Data encryption
(B). Data masking
(C). Data deduplication
(D). Data minimization
Answer: B
https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20a,partial%20data%20based%20on%20the%20user%E2%80%99s%20security%20permissions.
The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles
https://en.wikipedia.org/wiki/Data_masking

NO.210 A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on

their devices the following requirements must be met:
* Mobile device OSs must be patched up to the latest release
* A screen lock must be enabled (passcode or biometric)
* Corporate data must be removed if the device is reported lost or stolen Which of the following controls should the security engineer configure? (Select TWO)
(A). Containerization
(B). Storage segmentation
(C). Posturing
(D). Remote wipe
(E). Full-device encryption
(F). Geofencing

Answer: D,E

NO.211 A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?
(A). Developing an incident response plan
(B). Building a disaster recovery plan
(C). Conducting a tabletop exercise
(D). Running a simulation exercise
Answer: C

NO.212 A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?
(A). iPSec
(B). Always On
(C). Split tunneling
(D). L2TP
Answer: B

NO.213 A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?
(A). Segmentation
(B). Containment
(C). Geofencing
(D). Isolation
Answer: A

NO.214 A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same

one used by company staff as one of its approved third-party applications. After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?
(A). DLP
(B). SWG
(C). CASB
(D). Virtual network segmentation
Answer: A
E; Container security

NO.215 A user contacts the help desk to report the following:
Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
The user was able to access the Internet but had trouble accessing the department share until the next day.
The user is now getting notifications from the bank about unauthorized transactions.
Which of the following attack vectors was MOST likely used in this scenario?
(A). Rogue access point
(B). Evil twin
(C). DNS poisoning
(D). ARP poisoning
Answer: A
B

NO.216 DURING A SECURITY ASSESSMENT. A SECURITY ANALYST FINDS A FILE WITH OVERLY PERMISSIVE PERMISSION. WICH OF THE FOLLOWING TOOL WILL ALLOW THE ANALYST TO REDUCE THR PERMISSONFOR THE EXIXTING USER AND GROUPS AND REMOVE THE SET-USER-ID BIT FROM THE FILE?
(A). 1a
(B). Chflaga
(C). Chmod
(D). Leof
(E). aeuid
Answer: C

NO.217 A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data toss?
(A). Logic bomb
(B). Ransomware
(C). Fileless virus
(D). Remote access Trojans

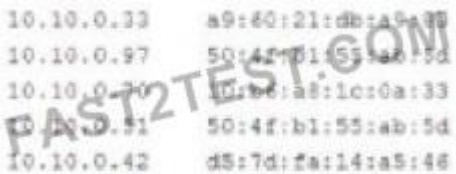
(E). Rootkit
Answer: A

NO.218 A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has Just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?
(A). Memory dumps
(B). The syslog server
(C). The application logs
(D). The log retention policy
Answer: B

NO.219 A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?
(A). Implement input validations
(B). Deploy MFA
(C). Utilize a WAF
(D). Configure HIPS
Answer: B C

NO.220 A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?
(A). Implement NAC.
(B). Implement an SWG.
(C). Implement a URL filter.
(D). Implement an MDM.
Answer: B

NO.221 A penetration tester successfully gained access ta a company's network, The investigating analyst detarmines malicious traffic connacted through the WAP despite filtering rules being in place, Logging in to the connected switch, the analyst sees the folowing in the ARP table:



Which of the following cid the penetration tester MOST liely use?
(A). ARP poisoning
(B). MAG eioning
(C). Man in the middle
(D). Evil twin
Answer: B C

NO.222 A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?
(A). Denial of service
(B). ARP poisoning
(C). Command injection
(D). MAC flooding
Answer: D

A

NO.223 To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive dat a. Which of the following cloud services would BEST accommodate the request?
(A). laas
(B). Paas
(C). Daas
(D). SaaS
Answer: D

B

NO.224 A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.
(A). validate the vulnerability exists in the organization's network through penetration testing
(B). research the appropriate mitigation techniques in a vulnerability database
(C). find the software patches that are required to mitigate a vulnerability
(D). prioritize remediation of vulnerabilities based on the possible impact.
Answer: D
The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat
https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

NO.225 An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became of aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?
(A). Reputation damage
(B). Identity theft
(C). Anonymlzation

(D). Interrupted supply chain
Answer: A

NO.226 In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?
(A). Identification
(B). Preparation
(C). Eradiction
(D). Recovery
(E). Containment
Answer: E

NO.227 Which of the following represents a biometric FRR?
(A). Authorized users being denied access
(B). Users failing to enter the correct PIN
(C). The denied and authorized numbers being equal
(D). The number of unauthorized users being granted access
Answer: A

NO.228 Which of the following will increase cryptographic security?
(A). High data entropy
(B). Algorithms that require less computing power
(C). Longer key longevity
(D). Hashing
Answer: C A

NO.229 A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?
(A). TFTP was disabled on the local hosts
(B). SSH was turned off instead of modifying the configuration file
(C). Remote login was disabled in the networkd.config instead of using the sshd.conf
(D). Network services are no longer running on the NAS
Answer: C

NO.230 Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).
(A). Offboarding
(B). Mandatory vacation
(C). Job rotation
(D). Background checks
(E). Separation of duties
(F). Acceptable use
Answer: B,C

NO.231 A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?
(A). Nmapn
(B). Heat maps
(C). Network diagrams
(D). Wireshark
Answer: C B

NO.232 After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?
(A). CASB
(B). VPC
(C). SWG
(D). CMS
Answer: A

NO.233 An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:
Check-in/checkout of credentials
The ability to use but not know the password
Automated password changes
Logging of access to credentials
Which of the following solutions would meet the requirements?
(A). OAuth 2.0
(B). Secure Enclave
(C). A privileged access management system
(D). An OpenID Connect authentication system
Answer: D C

NO.234 The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?
(A). A script kiddie
(B). Shadow IT
(C). Hacktivism
(D). White-hat
Answer: B

NO.235 After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for

forensic review?
(A). The vulnerability scan output
(B). The IDS logs
(C). The full packet capture data
(D). The SIEM alerts
Answer: A

NO.236 A security engineering installing A WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?
(A). A reverse proxy
(B). A decryption certificate
(C). A split-tunnel VPN
(D). Load-balanced servers
Answer: B

NO.237 A security analyst has identified malv/are spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT? A
(A). Review how the malware was introduced to the network
(B). Attempt to quarantine all infected hosts to limit further spread
(C). Create help desk tickets to get infected systems reimaged
(D). Update all endpomt antivirus solutions with the latest updates
Answer: C
B

NO.238 A forensic analyst needs to prove that data has not been tampered with since it was collected Which of the following methods will the analyst MOST likely use?
(A). Look for tampenng on the evidence collection bag
(B). Encrypt the collected data using asymmetric encryption
(C). Ensure proper procedures for chain of custody are being followed
(D). Calculate the checksum using a hashing algorithm
Answer: D

NO.239 A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account 'JHDoe' does not exist...
User account 'VMAdmin' does not exist...
User account 'tomcat' wrong password...
User account 'Admin' does not exist...
```


Which of the following MOST likely would have prevented the attacker from learning the service account name?
(A). Race condition testing
(B). Proper error handling
(C). Forward web server logs to a SIEM
(D). Input sanitization
Answer: B

NO.240 Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?
(A). Whaling
(B). Spam
(C). Invoice scam
(D). Pharming
Answer: D
Pharming: Phishing attempt to trick a user to access a different or fake website (usually by modifying hosts file)

NO.241 On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)
(A). Data accessibility
(B). Legal hold
(C). Cryptographic or hash algorithm
(D). Data retention legislation
(E). Value and volatility of data
(F). Right-to-audit clauses
Answer: E,F

NO.242 An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?
(A). On-path attack
(B). Protocol poisoning
(C). Domain hijacking
(D). Bluejacking
Answer: A

NO.243 A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporateowned devices to have access to the intranet but limit others to internet access only, Which of the following should the administrator recommend?
(A). 802.1X utilizing the current PKI infrastructure
(B). SSO to authenticate corporate users
(C). MAC address filtering with ACLS on the router
(D). PAM for user account management
Answer: A

NO.244 An analyst is reviewing logs associated with an attack. The logs indicate an attacker downloaded a malicious file that was quarantined by the AV solution. The attacker utilized a local non-administrative account to restore the malicious file to a new location. The file was then used by another process to execute a payload. Which of the following attacks did the analyst observe?
(A). Privilege escalation

(B). Request forgeries
(C). Injection
(D). Replay attack
Answer: A
C
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.[2] There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.[3] In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

NO.245 An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?
(A). Always On
(B). Remote access
(C). Site-to-site
(D). Full tunnel
Answer: C

NO.246 Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?
(A). TOTP
(B). Biometrics
(C). Kerberos
(D). LDAP
Answer: A

NO.247 Which of the following would detect intrusions at the perimeter of an airport?
(A). Signage
(B). Fencing
(C). Motion sensors
(D). Lighting
(E). Bollards
Answer: C

NO.248 An enterprise has hired an outside security firm lo conduct a penetration test on its network and applications, The enterprise provided the firm with access to a guest account. Which af the following BEST represents the type of testing that is being used?
(A). Black-box
(B). Red-team
(C). Gray-box

(D). Bug bounty
(E). White-box
Answer: C

NO.249 A security analyst is tasked with defining the "something you are" factor of the company's MFA settings. Which of the following is BEST to use to complete the configuration?
(A). Gait analysis
(B). Vein
(C). Soft token
(D). HMAC-based, one-time password
Answer: A

B

NO.250 Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?
(A). MOU
(B). ISA
(C). SLA
(D). NDA

Answer: A
A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.
https://csrc.nist.gov/glossary/term/interconnection_security_agreement

NO.251 A company uses wireless tor all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?
(A). A BPDU guard
(B). WPA-EAP
(C). IP filtering
(D). A WIDS
Answer: B
"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism." https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010. Source: https://jaimelightfoot.com/blog/comptia-security-wireless-security/ "EAP has been expanded into multiple versions." * "The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3." * "The Wi-Fi Alliance added EAP-FAST to its list of supported protocols for WPA/WPA2/WPA3." * "The Wi-Fi Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3." Excerpt From: Wm. Arthur Conklin. "CompTIA Security+ All-in-One Exam Guide

(Exam SY0-601))."

NO.252 The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?
(A). Install a NIDS device at the boundary.
(B). Segment the network with firewalls.
(C). Update all antivirus signatures daily.
(D). Implement application blacklisting
Answer: B

NO.253 A user reports falling for a phishing email to an analyst. Which of the following system logs would the analyst check FIRST?
(A). DNS
(B). Message gateway
(C). Network
(D). Authentication
Answer: B

A

NO.254 Which of the following would be used to find the MOST common web-application vulnerabilities?
(A). OWASP
(B). MITRE ATT&CK
(C). Cyber Kill Chain
(D). SDLC
Answer: A

NO.255 A junior security analyst iss conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple logtn entnes with the following text:

```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh
suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```


Which of Ihe following is the MOST likely attack conducted on the environment?
(A). Malicious script
(B). Privilege escalation
(C). Doman hijacking
(D). DNS poisoning
Answer: A

NO.256 Several employees have noticed other bystanders can clearly observe a terminal where passcodes are being entered, Which of the following can be eliminated with the use of a privacy screen?
(A). Shoulder surfing

(B). Spear phishing
(C). Impersonation attack
(D). Card cloning
Answer: A

NO.257 A administrator needs to allow mobele BYOD devices to access network resources, As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practces for authentication and infrastructure security? (Select TWO)
(A). Create a new network for the mobile devices and block the commurycaton to the intemal network and servers
(B). Use a captive portal for user authentication
(C). Authenticate users using OAuth for more resiliency.
(D). Implement SSO and allow communication to the intemal network.
(E). Use the existing network and allow communscation to the internal network and servers
(F). Use a new and updated RADIUS server to mamntain the best solution
Answer: B,C

NO.258 A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?
(A). Dumpster diving
(B). Shoulder surfing
(C). Information elicitation
(D). Credential harvesting
Answer: A D

NO.259 Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?
(A). WPA3
(B). AES
(C). RADIUS
(D). WPS
Answer: D

NO.260 After a recent security breach a security analyst reports that several admimstratrve usemames and passwords are being sent via cieartext across the network to access network devices over prot 23 Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configunng network devices?
(A). SSH
(B). SNMPv3
(C). SFTP
(D). Telnet
(E). FTP
Answer: A

NO.261 An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement?
(A). Proxy server
(B). WAF
(C). Load balancer
(D). VPN
Answer: B

NO.262 Which of the following describes the ability of code to target a hypervisor from inside
(A). Fog computing
(B). VM escape
(C). Software-defined networking
(D). Image forgery
(E). Container breakout
Answer: B
Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor.
https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs)%20running%20on%20that%20host.

NO.263 A major Clotting company recently lost 4 aege amount of propeetary wvformaton The security olficer must fied a solution t ensure frs never happens agan tht 8 the BEST tachrycal implementation tp prevent thes fom happening agai?
(A). Configure OLP soktons
(B). Disable peer-to-peer sharing
(C). Enable role-based access controls.
(D). Mandate job rotabon
(E). Implement content ters
Answer: A

NO.264 Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?
(A). GOPR
(B). CIS controls
(C). . ISO 27001
(D). Is0 37000
Answer: A

NO.265 Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?
(A). EOL
(B). SLA
(C). MOU
(D). EOSL
Answer: B

NO.266 An engineer is configuring AAA authentication on a Cisco MDS 9000 Series Switch. The LDAP server is located under the IP 10.10.2.2. The data sent to the LDAP server should be encrypted. Which command should be used to meet these requirements?
(A). ldap-server 10.10.2.2 key SSL_KEY
(B). ldap-server host 10.10.2.2 key SSL_KEY
(C). ldap-server 10.10.2.2 port 443
(D). ldap-server host 10.10.2.2 enable-ssl
Answer: D

NO.267 During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming convention and are not in the asset Inventory. WiFi access Is protected with 255-Wt encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode Which of the following should the administrator implement to find and remediate the Issue? (Select TWO).
(A). Check the SIEM for failed logins to the LDAP directory.
(B). Enable MAC filtering on the switches that support the wireless network.
(C). Run a vulnerability scan on all the devices in the wireless network
(D). Deploy multifactor authentication for access to the wireless network
(E). Scan the wireless network for rogue access points.
(F). Deploy a honeypot on the network
Answer: B,E

NO.268 A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?
(A). Hard token
(B). Retina scan
(C). SMS text
(D). Keypad PIN
Answer: B

NO.269 A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards. Which of the following is the MOST likely source of the breach?
(A). Side channel
(B). Supply chain
(C). Cryptographic downgrade
(D). Malware
Answer: C

B

NO.270 A manufacturer creates designs for very high security products that are required to be protected and controlled

(A). Session replay
(B). Evil twin
(C). Bluejacking
(D). ARP poisoning

Answer: B

NO.271 A security engineer is deploying a new wireless for a company. The company shares office space with multiple tenants. Which of the following should the engineer configured on the wireless network to ensure that confidential data is not exposed to unauthorized users?
(A). EAP
(B). TLS
(C). HTTPS
(D). AES
Answer: C

D

NO.272 A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?
(A). Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
(B). Install a sandbox to run the malicious payload in a safe environment
(C). Perform a traceroute to identify the communication path
(D). Use netstat to check whether communication has been made with a remote host
Answer: B

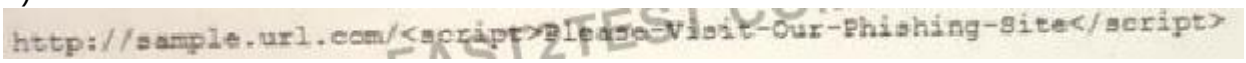
NO.273 To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?
(A). MaaS
(B). IaaS
(C). SaaS
(D). PaaS
Answer: D

C

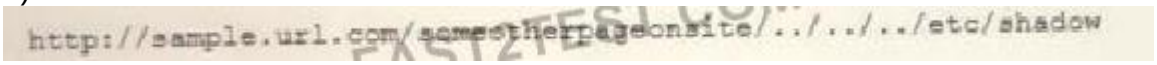
NO.274 A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email. The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations. Which of the following would address the CSO's concerns?
(A). SPF
(B). DMARC
(C). SSL
(D). DKIM
(E). TLS
Answer: E

NO.275 A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely

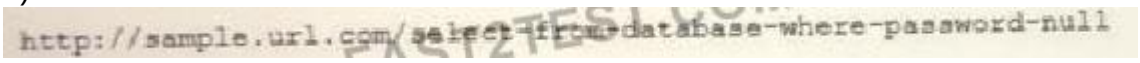
seeing?
A)



B)



C)



D)
(A). Option A
(B). Option B
(C). Option C
(D). Option D
Answer: B

NO.276 A company recently expenenced an attack dunng which #5 main website was directed to the atacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Vhich of the following snould the company Implement to prevent this type of attack from accurting in the future?
(A). IPSec
(B). SSL/TLS
(C). DNSSEC
(D). S/MIME
Answer: B C

NO.277 hich of the following ofien operaics in a clent-server architecture to act aa a sendoe repombory, providing entenprise consumers access to structured threal Intelligence data?
(A). STIX
(B). CIRT
(C). OSINT
(D). TARII
Answer: B

NO.278 During an intemal penetration test, a security analyst identified a network device that had accepted cleartext authentication and was configured with a default credential. Which of the following recommendations should the security analyst make to secure this device? A
(A). Configure SNMPv1.
(B). Configure SNMPv2c
(C). Configure SNMPv3.
(D). Configure the default community string.
Answer: D

NO.279 An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

(A). Using geographic diversity to have VPN terminators closer to end users
(B). Utilizing split tunneling so only traffic for corporate resources is encrypted
(C). Purchasing higher-bandwidth connections to meet the increased demand
(D). Configuring QoS properly on the VPN accelerators
Answer: D

B

NO.280 A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?
(A). Invalid trust chain
(B). Domain hijacking
(C). DNS poisoning
(D). URL redirection
Answer: C

NO.281 An organization is developing a plan in the event of a complete loss of critical systems and dat a. Which of the following plans is the organization MOST likely developing?
(A). Incident response
(B). Communications
(C). Disaster recovery
(D). Data retention
Answer: C

NO.282 An enterpnse has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?
(A). White-box
(B). Red-leam
(C). Bug bounty
(D). Gray-box
(E). Black-box
Answer: A

C

NO.283 Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?
(A). Transit gateway
(B). Cloud hot site
(C). Edge computing
(D). DNS sinkhole
Answer: A

NO.284 Which of the following relets to applications and systems that are used within an organization without consent or approval?
(A). Shadow IT
(B). OSINT
(C). Dark web
(D). Insider threats
Answer: A

NO.285 A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources.
Which of the following will the CISO MOST likely recommend to mitigate this risk?
(A). Upgrade the bandwidth available into the datacenter
(B). Implement a hot-site failover location
(C). Switch to a complete SaaS offering to customers
(D). Implement a challenge response test on all end-user queries
Answer: B

NO.286 An attacker replaces a digitally signed document with another version that foes unnoticed. Upon reviewing the document's contents, the author notices some additional verbaige that was not originally in the document but can't validate an integrity issue. Which of the following attacks was used?
(A). Cryptomalware
(B). Prepending
(C). Collision
(D). Phising
Answer: C

NO.287 A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?
(A). netstat
(B). net share
(C). netcat
(D). nbtstat
(E). net session
Answer: A

NO.288 A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?
(A). FDE
(B). NIDS
(C). EDR
(D). DLP
Answer: C

NO.289 A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?
(A). Session replay
(B). Evil twin
(C). Bluejacking
(D). ARP poisoning
Answer: B
https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack
One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

NO.290 Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)
(A). Alarms
(B). Signage
(C). Lighting
(D). Access control vestibules
(E). Fencing
(F). Sensors
Answer: D,E
Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure, Fencing=physical countermeasure and Sensors are either reactive or technical.
https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/

NO.291 The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?
(A). Geofencing
(B). Self-sovereign identification
(C). PKI certificates
(D). SSO
Answer: A B

NO.292 Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?
(A). Functional testing

(B). Stored procedures
(C). Elasticity
(D). Continuous integration
Answer: C

D

NO.293 A financial nstitution wauid like to stare its customer data in a coud but still allaw the data ta he accessed and manipulated while encrypted. Doing so would prevent the claud servine provider from heing adle ta decipher the data due ta its sensitivity. The financial institutan is not concernec about computational averheads and slow speeds, Which of the follawing cryotographic techniques would BEST meet the requirement?
(A). Asymmatric
(B). Symmetric
(C). Homeomorphic
(D). Ephemeral
Answer: A

C

NO.294 A security analyst is working on a project to implement a solution that monitors network communications and provides alerts when abnormal behavior is detected Which of the following is the security analyst MOST likely implementing?
(A). Vulnerability scans
(B). User behavior analysis
(C). Security orchestration, automation, and response
(D). Threat hunting
Answer: C
SOAR solutions automatically aggregate and validate data from various sources, including threat intelligence, security information and event management (SIEM), and user and entity behavior analytics (UEBA) tools. It helps make security operations centers (SOCs) intelligence-driven, providing the context needed to make informed decisions and accelerate detection and response.

NO.295 Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the internet No business emails were Identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounls Which of Ihe following would mitigate the issue?
(A). Complexity requirements
(B). Password history
(C). Acceptable use policy
(D). Shared accounts
Answer: C

B

NO.296 A company discovered that terabytes of data have been exfiltrated over the past year after an employee clicked on an email link. The threat continued to evolve and remain undetected until a security analyst noticed an abnormal amount of external connections when the employee was not working. Which of the following is the MOST likely threat actor?
(A). Shadow IT
(B). Script kiddies
(C). APT

(D). Insider threat

Answer: C

An APT attack is characterized by using toolkits to achieve a presence on a target network and then, instead of just moving to steal information, focusing on the long game by maintaining a persistent presence on the target network. The tactics, tools, and procedures of APTs are focused on maintaining administrative access to the target network and avoiding detection. Then, over the long haul, the attacker can remove intellectual property and more from the organization, typically undetected.

NO.297 Which of the following supplies non-repudiation during a forensics investigation?

(A). Dumping volatile memory contents first

(B). Duplicating a drive with dd

(C). Using a SHA-2 signature of a drive image

(D). Logging everyone in contact with evidence

(E). Encrypting sensitive data

Answer: C

NO.298 An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

(A). An external security assessment

(B). A bug bounty program

(C). A tabletop exercise

(D). A red-team engagement

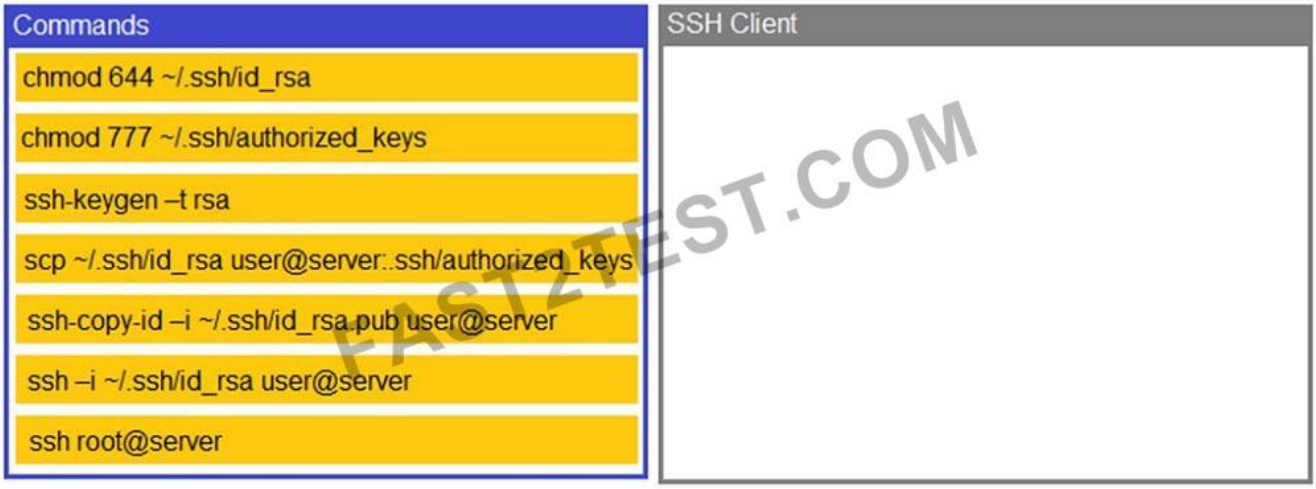
Answer: C

NO.299 A security engineer is setting up passwordless authentication for the first time.

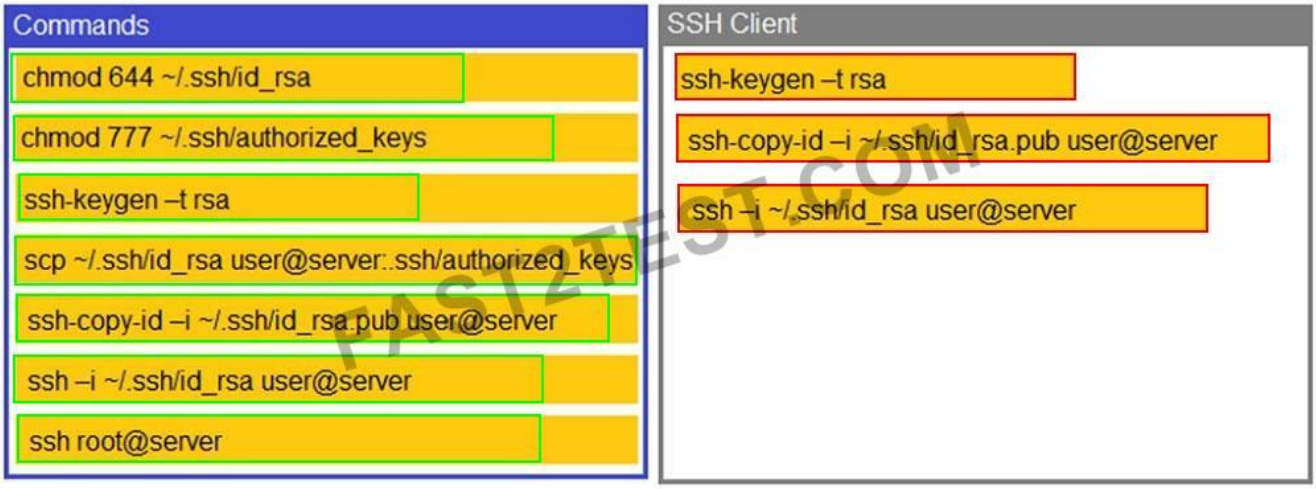
INSTRUCTIONS -

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



NO.300 A company Is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?
(A). Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network
(B). Change the password for the guest wireless network every month.
(C). Decrease the power levels of the access points for the guest wireless network.
(D). Enable WPA2 using 802.1X for logging on to the guest wireless network.
Answer: A

NO.301 A company has decovered unauthorized devices are using its WiFi network, and it wants to harden the access point to imporve security. Which f the following configuration shoujld an analysis enable To improve security? (Select TWO.)
(A). RADIUS
(B). PEAP
(C). WPS
(D). WEP-EKIP
(E). SSL
(F). WPA2-PSK
Answer: D,F

AF

NO.302 Which of tre following would BEST identity and remediate a catatoss event in an enterprise using third-pany, web-based services and file-sharing platanmns?
(A). SIEM
(B). CASE
(C). UTM
(D). EDR
Answer: B

NO.303 Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

(A). RTO
(B). MTBF
(C). MTTR
(D). RPO
Answer: C

NO.304 A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?
(A). SIEM
(B). DLP
(C). CASB
(D). SWG
Answer: C

NO.305 An attacker browses a company's online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?
(A). Hoax
(B). Reconnaissance
(C). Impersonation
(D). pretexting
Answer: A B

NO.306 A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?
(A). Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
(B). Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
(C). Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
(D). Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence
Answer: B
"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker." For purposes of knowing, https://security.opentext.com/tableau/hardware/details/t8u write blockers like this are the most popular hardware blockers

NO.307 The human resources department of a large online retailer has received multiple customer

complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?
(A). Baseline modification
(B). A fileless virus
(C). Tainted training data
(D). Cryptographic manipulation
Answer: C

NO.308 The website http://companywebsite.com requires users to provide personal information, including security question responses, for registration. Which of the following would MOST likely cause a data breach?
(A). Lack of input validation
(B). Open permissions
(C). Unsecure protocol
(D). Missing patches
Answer: C

NO.309 An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?
(A). A spear-phishing attack
(B). A watering-hole attack
(C). Typo squatting
(D). A phishing attack
Answer: B

NO.310 An engineer is setting up a VDI environment for a factory tocation, and the business wants to deploy a low-cost solution to enadle users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?
(A). Laptops
(B). Containers
(C). Thin clients
(D). Workstations

Answer: C

NO.311 An audit Identified PII being utilized In the development environment of a critical application. The Chief Privacy Officer (CPO) Is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific dat a. Which of the following should a security professional implement to BEST satisfy both the CPO's and the development team's requirements?
(A). Data anonymlzallon
(B). Data encryption
(C). Data masking
(D). Data tokenization
Answer: A

NO.312 A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:
* Protection from power outages
* Always-available connectivity In case of an outage
The owner has decided to implement battery backups for the computer equipment Which of the following would BEST fulfill the owner's second need?
(A). Lease a point-to-point circuit to provide dedicated access.
(B). Connect the business router to its own dedicated UPS.
(C). Purchase services from a cloud provider for high availability
(D). Replace the business's wired network with a wireless network
Answer: C

NO.313 The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schem a. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs Which of the following is the BEST solution to meet the requirement?
(A). Tokenization
(B). Masking
(C). Full disk encryption
(D). Mirroring
Answer: B

NO.314 An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?
(A). Information elicitation
(B). Type squatting
(C). Impersonation
(D). Watering-hole attack
Answer: D

NO.315 A Chief information Officer is concemed about employees using company-issued laptops to steal dala when accessing network shares Which of the following should the company implement?
(A). DLP
(B). CASB
(C). HIDS
(D). EDR
(E). UEFI
Answer: A

NO.316 A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting dat a. The following was observed running:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C | Format-Volume -DriveLetter C - FileSystemLabel "New"-FileSystem
NTFS - Full -Force -Confirm:$false |
```

Which of the following is the malware using to execute the attack?
(A). PowerShell
(B). Python
(C). Bash
(D). Macros
Answer: A

D

NO.317 The spread of misinformation sorrounding the outbreak of a bnovel virus on election day led to eligible voters chooseing not to take risk of goding to the polls. This is an exampla of:
(A). Prepending
(B). An influence compain
(C). A watering-hole attack.
(D). Intimidation.
(E). Information elicitation.
Answer: D

B

NO.318 During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?
(A). Check for any recent SMB CVEs
(B). Install AV on the affected server
(C). Block unneeded TCP 445 connections
(D). Deploy a NIDS in the affected subnet
Answer: C

NO.319 A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to implement a high availability pair to:
(A). ned that business may be negatecrease the mean time between failures.
(B). remove the single point of failure.
(C). cut down the mean time to repair,
(D). reduce the recovery time objective.
Answer: B

NO.320 A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?
(A). Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis.
(B). Restrict administrative privileges and patch all systems and applications.
(C). Rebuild all workstations and install new antivirus software.
(D). Implement application whitelisting and perform user application hardening.
Answer: A
The reason the company had to pay the ransom is because they did not have valid backups, otherwise they would have just restored their data. If your company just had to pay ransom and your boss says, "Don't let this happen again", what is the first thing you are going to do. The only action

after a ransomware attack is "restore from backup".

NO.321 A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?
(A). internet
(B). Screened Subnet
(C). VLAN segmentation
(D). Zero Trust
Answer: C

NO.322 A security analyst in a SOC has been tasked with onboarding a new network into the SIEM. Which of the following BEST describes the information that should feed into a SIEM solution in order to adequately support an investigation?
(A). Logs from each device type and security layer to provide correlation of events
(B). Only firewall logs since that is where attackers will most likely try to breach the network
(C). Email and web-browsing logs because user behavior is often the cause of security breaches
(D). NetFlow because it is much more reliable to analyze than syslog and will be exportable from every device
Answer: A

B

NO.323 A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?
(A). Netcat
(B). Netstat
(C). Nmap
(D). Nessus
Answer: B

NO.324 A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?
(A). Default system configuration
(B). Unsecure protocols
(C). Lack of vendor support
(D). Weak encryption
Answer: C

B

NO.325 A company recently experienced an inside attack using a corporate machine that resulted in data compromise. Analysis indicated an unauthorized change to the software circumvented technological protection measures, The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?
(A). HIPS
(B). Flm
(C). TPM

(D). DLP

Answer: C

https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation

NO.326 A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

(A). False rejection

(B). Cross-over error rate

(C). Efficacy rale

(D). Attestation

Answer: A

where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

NO.327 Which of the following uses SAML for authentication?

(A). TOTP

(B). Federation

(C). Kerberos

(D). HOTP

Answer: B

NO.328 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:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

(A). XSS attack

(B). SQLi attack

(C). Replay attack

(D). XSRF attack

Answer: B

NO.329 A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The fiieshare is located in a local data center. Which of the following should the security architect recommend to BEST meet the requirement?

(A). Fog computing and KVMs

(B). VDI and thin clients

(C). Private cloud and DLP

(D). Full drive encryption and thick clients

Answer: B

NO.330 A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).
(A). HIDS
(B). NIPS
(C). HSM
(D). WAF
(E). NAC
(F). NIDS
(G). Stateless firewall
Answer: B,D

NO.331 A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?
(A). S/MIME
(B). DLP
(C). IMAP
(D). HIDS
Answer: B
Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

NO.332 Which of the following BEST helps to demonstrate integrity during a forensic investigation?
(A). Event logs
(B). Encryption
(C). Hashing
(D). Snapshots
Answer: C

NO.333 A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?
(A). PCI DSS
(B). GDPR
(C). NIST
(D). ISO 31000
Answer: B

NO.334 An application owner has requested access for an external application to upload data from the central internal website without providing credentials at any point. Which of the following authentication methods should be configured to allow this type of integration access?
(A). OAuth
(B). SSO
(C). TACACS+

(D). Kerberos
Answer: B

NO.335 An organization has developed an application that needs a patch to fix a critical vulnerability In which of the following environments should the patch be deployed LAST?
(A). Test
(B). Staging
(C). Development
(D). Production
Answer: A D

NO.336 A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?
(A). Redundancy
(B). RAID 1+5
(C). Virtual machines
(D). Full backups
Answer: D

NO.337 As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?
(A). HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
(B). HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
(C). HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
(D). HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00
Answer: C

NO.338 A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?
(A). The DNS logs
(B). The web server logs
(C). The SIP traffic logs
(D). The SNMP logs
Answer: A

NO.339 Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)
(A). Block cipher
(B). Hashing
(C). Private key

(D). Perfect forward secrecy
(E). Salting
(F). Symmetric keys
Answer: B,C

NO.340 Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:
* There must be visibility into how teams are using cloud-based services.
* The company must be able to identify when data related to payment cards is being sent to the cloud.
* Data must be available regardless of the end user's geographic location
* Administrators need a single pane-of-glass view into traffic and trends.
Which of the following should the security analyst recommend?
(A). Create firewall rules to restrict traffic to other cloud service providers.
(B). Install a DLP solution to monitor data in transit.
(C). Implement a CASB solution.
(D). Configure a web-based content filter.
Answer: B

C

NO.341 hich of the following would be MOST effective to contain a rapidly spreading attack that is affecting a large number of organizations?
(A). Machine learning
(B). DNS sinkhole
(C). Blocklist
(D). Honeypot
Answer: C

B

NO.342 A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?
(A). Allow DNS access from the internet.
(B). Block SMTP access from the Internet
(C). Block HTTPS access from the Internet
(D). Block SSH access from the Internet.
Answer: D

NO.343 Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

(A). Production
(B). Test
(C). Staging
(D). Development
Answer: B

NO.344 An information security manager for an organization is completing a PCI DSS self-assessment for the first time. which of the is following MOST likely reason for this type of assessment?
(A). An international expansion project is currently underway.
(B). Outside consultants utilize this tool to measure security maturity.
(C). The organization is expecting to process credit card information.
(D). A government regulator has requested this audit to be completed
Answer: C

NO.345 A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an Item, the password for the wireless network is printed on the recent so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?
(A). WPA-EAP
(B). WEP-TKIP
(C). WPA-PSK
(D). WPS-PIN
Answer: A

NO.346 An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?
(A). Logic bomb
(B). Crypto malware
(C). Spyware
(D). Remote access Trojan
Answer: A
Logic bomb: 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.

NO.347 fier segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?
(A). A DMZ
(B). A VPN a
(C). A VLAN
(D). An ACL
Answer: D

NO.348 Which of the following will MOST likely adversely impact the operations of unpatched

traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)
(A). Cross-site scripting
(B). Data exfiltration
(C). Poor system logging
(D). Weak encryption
(E). SQL injection
(F). Server-side request forgery
Answer: D,E

DF

NO.349 In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?
(A). Identification
(B). Preparation
(C). Eradiction
(D). Recovery
(E). Containment
Answer: E
Isolation involves removing affected components from any environment the greater one. This can be anything from removing the server from the network after become the target of DoS attacks, to the point of placing applications in a VM sandbox outside the environment where the host usually runs. Whatever the situation, you'll want to make sure you don't there is another Interface between the affected component and the production network or the Internet.

NO.350 An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?
(A). The baseline
(B). The endpoint configurations
(C). The adversary behavior profiles
(D). The IPS signatures
Answer: C

A

NO.351 A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?
(A). WEP
(B). MSCHAP
(C). wes
(D). SAE
Answer: D

NO.352 Field workers in an organization are issued mobile phones on a daily basis All the work is

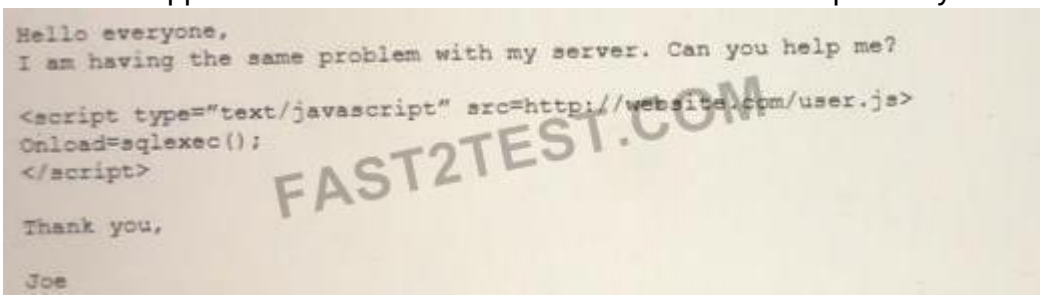
performed within one city and the mobile phones are not used for any purpose other than work The organization does not want these pnones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the pnones do not need to be reissued every day Qven the conditions described, which of the following technologies would BEST meet these requirements'
(A). Geofencing
(B). Mobile device management
(C). Containenzation
(D). Remote wiping
Answer: B

NO.353 Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?
(A). To avoid data leakage
(B). To protect surveillance logs
(C). To ensure availability
(D). To facilitate third-party access
Answer: C

A

NO.354 A routine audit of medical billing claims revealed that several claims were submitted without the subscriber's knowledge. A review of the audit logs for the medical billing company's system indicated a company employee downloaded customer records and adjusted the direct deposit information to a personal bank account. Which of the following does this action describe?
(A). Insider threat
(B). Social engineering
(C). Third-party risk
(D). Data breach
Answer: A

NO.355 An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:



Which of the following BEST describes the attack that was attempted against the forum readers?
(A). SOU attack
(B). DLL attack
(C). XSS attack
(D). API attack
Answer: C
Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted website for the consumption of other valid users. The most

common example can be found in bulletin-board websites which provide web based mailing list-style functionality. https://owasp.org/www-community/attacks/xss/
https://www.acunetix.com/websitesecurity/cross-site-scripting/

NO.356 A new company wants to avoid channel interference when building a WLAN. The company needs to know the radio frequency behavior, identify dead zones, and determine the best place for access points. Which of the following should be done FIRST?
(A). Configure heat maps.
(B). Utilize captive portals.
(C). Conduct a site survey.
(D). Install Wi-Fi analyzers.
Answer: A

NO.357 Security analysts are conducting an investigation of an attack that occurred inside the organization's network. An attacker was able to connect network traffic between workstation throughout the network. The analysts review the following logs:

VLAN	Address
1	0007.1e5d.3213
1	002a.7d.44.8801
1	0011.aab4.344d

The layer 2 address table has hundred of entries similar to the ones above. Which of the following attacks has MOST likely occurred?
(A). SQL injection
(B). DNS spoofing
(C). MAC flooding
(D). ARP poisoning
Answer: D

C

NO.358 After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:
(A). privilege escalation
(B). footprinting
(C). persistence
(D). pivoting.
Answer: A

D

NO.359 A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?
(A). Code signing
(B). Fuzzing

(C). Manual code review
(D). Dynamic code analysis
Answer: D

B

NO.360 Which of the following would produce the closet experience of responding to an actual incident response scenario?
(A). Lessons learned
(B). Simulation
(C). Walk-through
(D). Tabletop
Answer: B

NO.361 Server administrator want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently acress a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availiability. Which of the following should administrator configure to maximize system availability while efficiently utilizing available computing power?
(A). Dynamic resource allocation
(B). High availability
(C). Segmentation
(D). Container security
Answer: C

A

* **NO.362** Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?
(A). Hashing
(B). DNS sinkhole
(C). TLS inspection
(D). Data masking
Answer: B

NO.363 An end user reoorts a computer has been acting slower than normal for a few weeks, During an investigation, an analyst determines the system 3 sending the users email address and a ten-cigit number ta an IP ackiress ance a day. The anly resent (ag entry regarding the user's computer is the fallowing:

Which of the following is the MOST likely cause of the issue?
(A). The end user purchased anc installed 2 PUP from a wab browser.
(B). bot on the cornputer is rule forcing passwords aguinsl vy websile.
(C). A hacker Is attempting to ex'itrate sens tve cata.
(D). Ransomwere is communicating with 8 commard-and-contral server.
Answer: A

NO.364 The cost of removable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratories to make data transfers easier and more secure.
The Chief Security Officer (CSO) has several concerns about proprietary data being exposed once the interconnections are established. Which of the following security features should the network administrator implement to prevent unwanted data exposure to users in partner laboratories?
(A). VLAN zoning with a file-transfer server in an external-facing zone
(B). DLP running on hosts to prevent file transfers between networks
(C). NAC that permits only data-transfer agents to move data between networks
(D). VPN with full tunneling and NAS authenticating through the Active Directory
Answer: B D

NO.365 Which of the following is the BEST action to foster a consistent and auditable incident response process?
(A). Incent new hires to constantly update the document with external knowledge.
(B). Publish the document in a central repository that is easily accessible to the organization.
(C). Restrict eligibility to comment on the process to subject matter experts of each IT silo.
(D). Rotate CIRT members to foster a shared responsibility model in the organization.
Answer: B D

NO.366 Which of the following is used to ensure that evidence is admissible in legal proceedings when it is collected and provided to the authorities?
(A). Chain of custody
(B). Legal hold
(C). Event log
(D). Artifacts
Answer: A

NO.367 A security analyst has identified malware spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?
(A). Review how the malware was introduced to the network.
(B). Attempt to quarantine all infected hosts to limit further spread.
(C). Create help desk tickets to get infected systems reimaged.
(D). Update all endpoint antivirus solutions with the latest updates.
Answer: B

NO.368 The concept of connecting a user account across the systems of multiple enterprises is BEST known as:
(A). federation.
(B). a remote access policy.
(C). multifactor authentication.
(D). single sign-on.
Answer: D A

NO.369 Which of the following conditions impacts data sovereignty?

(A). Rights management
(B). Criminal investigations
(C). Healthcare data
(D). Intemational operations
Answer: D

NO.370 A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?
(A). Implement a full system upgrade
(B). Perform a physical-to-virtual migration
(C). Install uninterruptible power supplies
(D). Purchase cybersecurity insurance
Answer: B

NO.371 A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.
An incident responder learns the following information:
The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.
Which of the following is the MOST likely root cause?
(A). HTTPS sessions are being downgraded to insecure cipher suites
(B). The SSL inspection proxy is feeding events to a compromised SIEM
(C). The payment providers are insecurely processing credit card charges
(D). The adversary has not yet established a presence on the guest WiFi network
Answer: C

NO.372 A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?
(A). RA
(B). OcsP
(C). CRL
(D). CSR
Answer: C

NO.373 A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?
(A). Hoaxes

(B). SPIMs
(C). Identity fraud
(D). Credential harvesting
Answer: A
Hoax
A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.
Identity theft
Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.
Credential Harvesting
Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

NO.374 Which of the following is a difference between a DRP and a BCP?
(A). A BCP keeps operations running during a disaster while a DRP does not.
(B). A BCP prepares for any operational interruption while a DRP prepares for natural disasters.
(C). BCP is a technical response to disasters while a DRP is operational.
(D). A BCP is formally written and approved while a DRP is not.
Answer: C

NO.375 Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?
(A). Cloud control matrix
(B). Reference architecture
(C). NIST RMF
(D). CIS Top 20
Answer: C

NO.376 A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?
(A). # iptables -t mangle -X
(B). # iptables -F
(C). # iptables -Z
(D). # iptables -P INPUT -j DROP
Answer: D
A

NO.377 Which of the following would MOST likely support the integrity of a voting machine?
(A). Asymmetric encryption
(B). Blockchain

(C). Transport Layer Security
(D). Perfect forward secrecy
Answer: D B

NO.378 A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?
(A). A packet capture
(B). A user behavior analysis
(C). Threat hunting
(D). Credentialed vulnerability scanning
Answer: C

NO.379 A security analyst wants to fingerpnnt a web server Which of the following tools will the security analyst MOST likely use to accomplish this task?
(A). nmap -p1-65S35 192.168.0.10
(B). dig 192.168.0.10
(C). cur1 --htad http://192.168.0.10
(D). ping 192.168.0.10
Answer: C
HTTP/1.1 301 Moved Permanently
Server: cloudflare
Date: Thu, 01 Sep 2022 22:36:50 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Location: https://1.1.1.1/
CF-RAY: 74417cb04d6b9a50-MFE

NO.380 An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?
(A). Data protection officer
(B). Data owner
(C). Backup administrator
(D). Data custodian
(E). Internal auditor

Answer: D

NO.381 Asecurity engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses Which of the following will the engineer MOST likely recommend?
(A). Acontent filter
(B). AWAF
(C). Anext-generation firewall
(D). An IDS

Answer: C

NO.382 A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?
(A). Man-in- the middle
(B). Spear-phishing
(C). Evil twin
(D). DNS poising
Answer: D
DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).
https://en.wikipedia.org/wiki/DNS_spoofing

NO.383 Which of the following control types fixes a previously identified issue and mitigates a risk?
(A). Detective
(B). Corrective
(C). Preventative
(D). Finalized
Answer: B

NO.384 A security administrator suspects an employee has been emailing proprietary information to a competitor.
Company policy requires the administrator to capture an exact copy of the employee's hard disk.
Which of the following should the administrator use?
(A). dd
(B). chmod
(C). dnsenum
(D). logger
Answer: A

NO.385 A company is under investigation for possible fraud. As part of the investigation. the authorities need to review all emails and ensure data is not deleted.
Which of the following should the company implement to assist in the investigation?
(A). Legal hold
(B). Chain of custody
(C). Data loss prevention
(D). Content filter
Answer: A

NO.386 A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this

process?
(A). Continuous delivery
(B). Continuous integration
(C). Continuous validation
(D). Continuous monitoring
Answer: B

NO.387 A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?
(A). 0
(B). 1
(C). 5
(D). 6
Answer: B D

NO.388 A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)
(A). DNSSEC
(B). Reverse proxy
(C). VPN concentrator
(D). PKI
(E). Active Directory
(F). RADIUS
Answer: E,F

NO.389 A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?
(A). IaaS
(B). PasS
(C). MaaS
(D). SaaS
Answer: D

NO.390 An organidation recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation, a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved. Which of the following attacks MOST likely explains the behavior?
(A). Birthday
(B). Rainbow table
(C). Impersonation
(D). Whaling
Answer: C D

NO.391 The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).
(A). Geolocation
(B). Time-of-day restrictions
(C). Certificates
(D). Tokens
(E). Geotagging
(F). Role-based access controls
Answer: A,E

AB

NO.392 A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?
(A). An NGFW
(B). A CASB
(C). Application whitelisting
(D). An NG-SWG
Answer: B

NO.393 A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
The attackers are using the targeted shoppers' credit card information to make online purchases.
Which of the following attacks is the MOST probable cause?
(A). Identity theft
(B). RFID cloning
(C). Shoulder surfing
(D). Card skimming
Answer: D

NO.394 A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?
(A). Automated failover
(B). Containerization
(C). CASB
(D). SWG
Answer: B
Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

NO.395 A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?
(A). A service-level agreement
(B). A business partnership agreement
(C). A SOC 2 Type 2 report
(D). A memorandum of understanding
Answer: A

NO.396 A financial nstitution wauid like to stare its customer data in a coud but still allaw the data ta he accessed and manipulated while encrypted. Doing so would prevent the claud servine provider from heing adle ta decipher the cata due ta its sensitivity. The financial institutan is not concernec about computational averheads and slow speeds, Which of the follawing cryotographic techniques would BEST meet the requirement?
(A). Asymmatric
(B). Symmetric
(C). Homeomorph
(D). Ephemeral
Answer: B C

NO.397 The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?
(A). Requiring all new, on-site visitors to configure their devices to use WPS
(B). Implementing a new SSID for every event hosted by the college that has visitors
(C). Creating a unique PSK for every visitor when they arrive at the reception area
(D). Deploying a captive portal to capture visitors' MAC addresses and names
Answer: D

NO.398 A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?
(A). Ipconfig
(B). ssh
(C). Ping
(D). Netstat
Answer: D
https://www.sciencedirect.com/topics/computer-science/listening-port

NO.399 Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?
(A). SSAE SOC 2
(B). PCI DSS
(C). GDPR
(D). ISO 31000

Answer: C

NO.400 During an incident response, an analyst applied rules to all inbound traffic on the border firewall and implemented ACLs on each critical server Following an investigation, the company realizes it is still vulnerable because outbound traffic is not restricted and the adversary is able lo maintain a presence in the network. In which of the following stages of the Cyber Kill Chain is the adversary currently operating?
(A). Reconnaissance
(B). Command and control
(C). Actions on objective
(D). Exploitation

Answer: B

NO.401 A company is receiving emails with links to phishing sites that look very similar to the company's own website address and content. Which of the following is the BEST way for the company to mitigate this attack?
(A). Create a honeynet to trap attackers who access the VPN with credentials obtained by phishing.
(B). Generate a list of domains similar to the company's own and implement a DNS sinkhole for each.
(C). Disable POP and IMAP on all Internet-facing email servers and implement SMTPS.
(D). Use an automated tool to flood the phishing websites with fake usernames and passwords.
Answer: B

NO.402 A security engineer needs to Implement the following requirements:
* All Layer 2 switches should leverage Active Directory tor authentication.
* All Layer 2 switches should use local fallback authentication If Active Directory Is offline.
* All Layer 2 switches are not the same and are manufactured by several vendors.
Which of the following actions should the engineer take to meet these requirements? (Select TWO).
Implement RADIUS.
(A). Configure AAA on the switch with local login as secondary
(B). Configure port security on the switch with the secondary login method.
(C). Implement TACACS+
(D). Enable the local firewall on the Active Directory server.
(E). Implement a DHCP server
Answer: A,B
Radius ve AAA

NO.403 A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?
(A). Content filter
(B). SIEM
(C). Firewall rules
(D). DLP
Answer: B
C

NO.404 Which of the following is a policy that provides a greater depth of knowldge across an

organization?
(A). Asset manahement policy
(B). Separation of duties policy
(C). Acceptable use policy
(D). Job Rotation policy
Answer: C

D

NO.405 Which of the following stores data directly on devices with limited processing and storage capacity?
(A). Thin client
(B). Containers
(C). Edge
(D). Hybrid cloud
Answer: A

NO.406 A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?
(A). .pfx
(B). .csr
(C). .pvk
(D). .cer
Answer: A

NO.407 A mae Clotting company recently lost 4 aege amount of propeetary wvformaton The security olficer must fied a solution t ensure frs never happens agan tht 8 the BEST tachrycal implementation tp prevent thes fom happening agai?
(A). Configure OLP soktons
(B). Disable peer-to-peer sharing
(C). Enable role-based access controls.
(D). Mandate job rotabon
(E). Implement content ters
Answer: B

A

NO.408 An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?
(A). Zero-day
(B). Default permissions
(C). Weak encryption
(D). Unsecure root accounts
Answer: A

NO.409 hich of the folowing would be BEST for a technician to review to determing the total figk an organizalion can bear when assessing a "cloud-firet" adoption sraiegy?
(A). Risk matrix
(B). Risk tolerance
C Risk register

(C). Risk appetite
Answer: B

NO.410 The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?
(A). Security awareness training
(B). Frequency of NIDS updates
(C). Change control procedures
(D). EDR reporting cycle

Answer: A

NO.411 A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?
(A). It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
(B). It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
(C). It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
(D). It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach
Answer: A

NO.412 A local server recently crashed, and the team is attempting to restore the server from a backup. During the restore process, the team notices the file size of each daily backup is large and will run out of space at the current rate. The current solution appears to do a full backup every night. Which of the following would use the LEAST amount of storage space for backups?
(A). Aweekly, incremental backup with daily differential backups
(B). Aweekly, full backup with daily snapshot backups
(C). Aweekly, full backup with daily differential backups
(D). Aweekly, full backup with daily incremental backups
Answer: C

NO.413 A security administrator is analyzing the corporate wireless network The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports Which of the following attacks in happening on the corporate network?
(A). Man in the middle
(B). Evil twin
(C). Jamming
(D). Rogue access point
(E). Disassociation
Answer: B

NO.414 An analyst is working on an email security incident in which the target opened an

attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?
(A). Apply a DLP solution.
(B). Implement network segmentation
(C). Utilize email content filtering,
(D). isolate the infected attachment.
Answer: B

NO.415 ecent changes toa company's BYOD policy require all personal mobile devices to use a two-factor authentication method that Is not something you know or have. Which of the following will meet this requirement?
(A). Facial recognition
(B). Six-digit PIN
(C). PKI certificate
(D). Smart card
Answer: C

NO.416 A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)
(A). Auto-update
(B). HTTP headers
(C). Secure cookies
(D). Third-party updates
(E). Full disk encryption
(F). Sandboxing
(G). Hardware encryption
Answer: A,G

NO.417 Which of the following types of attacks is specific to the individual it targets?
(A). Whaling
(B). Pharming
(C). Smishing
(D). Credential harvesting
Answer: A

NO.418 A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?
(A). The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
(B). All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
(C). Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
(D). MDMs typically will not support heterogeneous deployment environments, so multiple MDMs

will need to be installed and configured.
Answer: C

NO.419 Which of the following cloud models provides clients with servers, storage, and networks but nothing else?
(A). SaaS
(B). PaaS
(C). IaaS
(D). DaaS
Answer: C

NO.420 Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?
(A). Identify theft
(B). Data loss
(C). Data exfiltration
(D). Reputation

Answer: D

C

NO.421 A technician was dispatched to complete repairs on a server in a data center. While locating the server, the technician entered a restricted area without authorization. Which of the following security controls would BEST prevent this in the future?
(A). Use appropriate signage to mark all areas.
(B). Utilize cameras monitored by guards.
(C). Implement access control vestibules.
(D). Enforce escorts to monitor all visitors.
Answer: C

NO.422 Which of the following is an example of risk avoidance?
(A). Installing security updates directly in production to expedite vulnerability fixes
(B). Buying insurance to prepare for financial loss associated with exploits
(C). Not installing new software to prevent compatibility errors
(D). Not taking preventive measures to stop the theft of equipment
Answer: C

NO.423 A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?
(A). logger
(B). Metasploit
(C). tcpdump
(D). netstat
Answer: D

NO.424 A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage

displaying incorrect information. A quick nslookup search shows hitps://;www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?
(A). DoS attack
(B). ARP poisoning
(C). DNS spoofing
(D). NXDOMAIN attack
Answer: C

NO.425 In which of the following common use cases would steganography be employed?
(A). Obfuscation
(B). Integrity
(C). Non-repudiation
(D). Blockchain
Answer: A

NO.426 A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?
(A). A reverse proxy
(B). A decryption certificate
(C). A spill-tunnel VPN
(D). Load-balanced servers
Answer: B

NO.427 Asecurity analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS. Which of the following is the MOST likely attack type?
(A). Request forgery
(B). Session replay
(C). DLL injection
(D). Shimming
Answer: A D

NO.428 A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).
(A). Password and security question
(B). Password and CAPTCHA
(C). Password and smart card
(D). Password and fingerprint
(E). Password and one-time token
(F). Password and voice
Answer: C,D

NO.429 An IT manager is estimating the mobile device budget for the upcoming year Over the last five years, the number of devices that were replaced due to loss damage or theft steadily increased

by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?
(A). ALE
(B). ARO
(C). RPO
(D). SLE
Answer: A

B

NO.430 An information security policy states that separation of duties is required for all highly sensitive database changes that involve customers' financial dat a. Which of the following will this be BEST to prevent?
(A). Least privilege
(B). An insider threat
(C). Adata breach
(D). A change control violation

Answer: B

NO.431 A security engi is cor that the gy tor on endpoints ts too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key Mes and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?
(A). NIDS
(B). HIPS
(C). AV
(D). NGFW
Answer: A

B

NO.432 Which of the following holds staff accountable while escorting unathorized personal?
(A). Locks
(B). Badges
(C). Cameras
(D). Visitor logs
Answer: D

B

NO.433 An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).
(A). Corrective
(B). Deterrent
(C). Preventive
(D). Mandatory vacations
(E). Job rotation
(F). Separation of duties
Answer: D,E

NO.434 A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same

user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?
(A). Network location
(B). Impossible travel time
(C). Geolocation
(D). Geofencing
Answer: D

B

NO.435 A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST these requirement?
(A). RA
(B). OCSP
(C). CRL
(D). CSR
Answer: C

NO.436 A security analyst is designing the appropnate controls to limit unauthorized access to a physical site The analyst has a directive to utilize the lowest possible budget Which of the following would BEST meet the requirements?
(A). Preventive controls
(B). Compensating controls
(C). Deterrent controls
(D). Detective controls
Answer: C
Deterrent makes sense on further thought. The question just states unauthorized access. It doesn't state the intent of any unauthorized intruders. Deterrence is designed to reduce the occurrence of unintentional bystanders or unmotivated malicious agents from entering the site. Should the agent be motivated enough, a preventative measure is needed. But again, the question doesn't list intentions. Therefore this method works to limit the number of unauthorized visitors by weeding out everyone but the motivated, and the truly stupid.

NO.437 A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.
Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads.
Which of the following BEST describe this type of attack? (Choose two.)
(A). DoS
(B). SSL stripping
(C). Memory leak
(D). Race condition
(E). Shimming

(F). Refactoring
Answer: A,D

AC

NO.438 Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).
(A). A Production
(B). Test
(C). Research and development
(D). PoC
(E). UAT
(F). SDLC
Answer: B,E

NO.439 A company wants to improve end users experiences when they tog in to a trusted partner website The company does not want the users to be issued separate credentials for the partner website Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner's website?
(A). Directory service
(B). AAA server
(C). Federation
(D). Multifactor authentication
Answer: C

NO.440 A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?
(A). Configure the DLP policies to allow all PII
(B). Configure the firewall to allow all ports that are used by this application
(C). Configure the antivirus software to allow the application
(D). Configure the DLP policies to whitelist this application with the specific PII
(E). Configure the application to encrypt the PII
Answer: D

NO.441 A security analyst Is reviewing the following output from a system:

Which of the following is MOST likely being observed?
(A). ARP polsoning
(B). Man in the middie
(C). Denial of service
(D). DNS poisoning
Answer: C

NO.442 While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?
(A). Revoke the code signing certificate used by both programs.
(B). Block all unapproved file hashes from installation.
(C). Add the accounting application file hash to the allowed list.
(D). Update the code signing certificate for the approved application.
Answer: C

NO.443 A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us
Which of the following application attacks is being tested?
(A). Pass-the-hash
(B). Session replay
(C). Object deference
(D). Cross-site request forgery
Answer: B

NO.444 A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?
(A). Vishing
(B). Phishing

(C). Spear phishing
(D). Whaling
Answer: A

NO.445 A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?
(A). BYOD
(B). VDI
(C). COPE
(D). CYOD
Answer: A

D

NO.446 A company needs to validate its updated incident response plan using a real-world scenario that will test decision points and relevant incident response actions without interrupting daily operations. Which of the following would BEST meet the company's requirements?
(A). Red-team exercise
(B). Capture-the-flag exercise
(C). Tabletop exercise
(D). Phishing exercise
Answer: C

NO.447 A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?
(A). Containerization
(B). Geofencing
(C). Full-disk encryption
(D). Remote wipe
Answer: C

A

NO.448 ihic ofthe lowing iste BEST resnon to meitsin frciona ani SSUES Rane ETS or cricai?
(A). To provide data to quantify risk based on the organization's systems
(B). To keep all software and hardware fully patched for known vulnerabilities
(C). To only allow approved, organization-owned devices onto the business network
(D). To standardize by selecting one laptop model for all users in the organization
Answer: A

B

NO.449 After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:
(A). privilege escalation
(B). footprinting
(C). persistence
(D). pivoting.

Answer: A

D

NO.450 Developers are writing code and merging it into shared repositones several times a day, where it is tested automabecally. Which of the following concepts does this BEST represent?
(A). Functional testing
(B). Stored procedures
(C). Elasticity
(D). Continuous integration
Answer: C

D

NO.451 A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?
(A). Predictability
(B). Key stretching
(C). Salting
(D). Hashing
Answer: C

NO.452 Which of the fofowing should an organization conskier implementing in the event executives need to speak to the media after a publicized data breach?
(A). incident response pian
(B). Business continuity plan
(C). Communication pian
(D). Disaster recovery plan
Answer: C

NO.453 A security administrator checks the table of a network switch, which shows the following output:
Which of the following is happening to this switch?
(A). MAC Flooding
(B). DNS poisoning
(C). MAC cloning
(D). ARP poisoning
Answer: A

NO.454 A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices Which of the following is a cost-effective approach to address these concerns?
(A). Enhance resiliency by adding a hardware RAID.
(B). Move data to a tape library and store the tapes off-site
(C). Install a local network-attached storage.
(D). Migrate to a cloud backup solution
Answer: D

NO.455 A ecurily analyst b concemed alout iratic initiated to he dark web fom the corporate LAN. Which of the folowing motworks should he analyst monior?
(A). SFTP
(B). AS
(C). Tor
(D). LoC
Answer: C

NO.456 A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?
(A). Automated information sharing
(B). Open-source intelligence
(C). The dark web
(D). Vulnerability databases
Answer: C

NO.457 After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session Which of the following types of attacks has occurred?
(A). Privilege escalation
(B). Session replay
(C). Application programming interface
(D). Directory traversal
Answer: A

B

NO.458 A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?
(A). Physical
(B). Detective
(C). Preventive
(D). Compensating
Answer: D

* **NO.459** A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?
(A). TOP
(B). IMAP
(C). HTTPS
(D). S/MIME
Answer: D

NO.460 The new Chief Executive Officer (CEO) of a large company has announced a partnership with

a vendor that will provide multiple collaboration applications t make remote work easier. The company has a geographically dispersed staff located in numerous remote offices in different countries. The company's IT administrators are concerned about network traffic and load if all users simultaneously download the application. Which of the following would work BEST to allow each geographic region to download the software without negatively impacting the corporate network?
(A). Update the host IDS rules.
(B). Enable application whitelisting.
(C). Modify the corporate firewall rules.
(D). Deploy all applications simultaneously.

Answer: B

NO.461 A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?
(A). DNS sinkholding
(B). DLP rules on the terminal
(C). An IP blacklist
(D). Application whitelisting
Answer: D

NO.462 it a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?
(A). Pertect forward secrecy
(B). Eiliptic-curve cryptography
(C). Key stretching
(D). Homomorphic encryption
Answer: B

A

NO.463 A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?
(A). Enforcing encryption
(B). Deploying GPOs
(C). Removing administrative permissions
(D). Applying MDM software
Answer: D
MDM stands for Mobile Device Management, is software that assists in the implementation of the process of managing, monitoring, and securing several mobile devices such as tablets, smartphones, and laptops used in the organization to access the corporate information.

NO.464 Which of the following employee roles is responsible for protecting an organization's collected personal information?
(A). CTO
(B). DPO
(C). CEO
(D). DBA

Answer: B
Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization's overall data privacy policies.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=Many%20companies%20also%20have%20a,organization's%20overall%20data%20privacy%20policies.

NO.465 Which of the following controls is used to make an organization initially aware of a data compromise?
(A). Protective
(B). Preventative
(C). Corrective
(D). Detective
Answer: D
https://purplesec.us/security-controls/

NO.466 An untrusted SSL certificate was discovered during the most recent vulnerability scan. A security analyst determines the certificate is signed properly and is a valid wildcard. This same certificate is installed on other company servers without issue. Which of the following is the MOST likely reason for this finding?
(A). The required intermediate certificate is not loaded as part of the certificate chain.
(B). The certificate is on the CRL and is no longer valid.
(C). The corporate CA has expired on every server, causing the certificate to fail verification.
(D). The scanner is incorrectly configured to not trust this certificate when detected on the server.
Answer: A

NO.467 A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?
(A). NIC Teaming
(B). Port mirroring
(C). Defense in depth
(D). High availability
(E). Geographic dispersal
Answer: C

NO.468 A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?
(A). SSL
(B). FTP
(C). SNMP
(D). TLS
Answer: D

NO.469 Whiich of the following Gieuster recovery tests ie the LEAST time coneuntng for tie easier recovery tearm?
(A). Tabletop
(B). Parallel
(C). Full interruption
(D). Simulation
Answer: A

* **NO.470** Which of the following identifies the point in time when an organization will recover data in the event of an outage?
(A). ALE
(B). RPO
(C). MTBF
(D). ARO
Answer: B

NO.471 A security analyst is receiving several alerts per user and is trying to determine If various logins are malicious. The security analyst would like to create a baseline of normal operations and reduce 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.
Answer: D

NO.472 A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?
(A). CASB
(B). SWG
(C). Containerization
(D). Automated failover
Answer: C
Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

NO.473 A retail company that is launching @ new website to showcase the company's product line and other information for online shoppers registered the following URLs:
* www companysite com
* shop companysite com
* about-us companysite com
contact-us. companysite com
secure-logon companysite com
Which of the following should the company use to secure its website if the company is concemed with convenience and cost?

(A). A self-signed certificate
(B). A root certificate
(C). A code-signing certificate
(D). Awildcard certificate
(E). An extended validation certificate
Answer: B

NO.474 Business partners are working on a secunty mechanism lo validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign encrypt, and decrypt transaction files. Which of the following is the BEST solution to adopt?
(A). PKI
(B). Blockchain
(C). SAML
(D). OAuth
Answer: A

B

NO.475 Which of the following describes the exploitation of an interactive process to gain access to restncted areas?
(A). Persistence
(B). Buffer overflow
(C). Privilege escalation
(D). Pharming
Answer: C
https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%20an%20application%20or%20user

NO.476 A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?
(A). Repository transaction logs
(B). Common Vulnerabilities and Exposures
(C). Static code analysis
(D). Non-credentialed scans
Answer: B

C

NO.477 When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?
(A). Acceptance
(B). Mitigation
(C). Avoidance
(D). Transference
Answer: D

NO.478 While investigating a recent security incident, a security analyst decides to view all network

connections on a particular server, Which of the following would provide the desired information?
(A). arp
(B). nslookup
(C). netstat
(D). nmap
Answer: C

NO.479 Which of the following describes the BEST approach for deploying application patches?
(A). Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
(B). Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
(C). Test the patches m a test environment apply them to the production systems and then apply them to a staging environment
(D). Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment
Answer: A
https://oroinc.com/b2b-ecommerce/blog/testing-and-staging-environments-in-ecommerce-implementation/

NO.480 A security analyst has been reading about a newly discovered cyberattack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?
(A). Security research publications
(B). The MITRE ATT&CK framework
(C). The Diamond Model of Intrusion Analysis
(D). The Cyber Kill Chain

Answer: B

NO.481 A security administrator has discovered that workstations on the LAN are becoming infected with malware. The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?
(A). Forward proxy
(B). HIDS
(C). Awareness training
(D). A jump server
(E). IPS
Answer: D

B

NO.482 A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?
(A). PCI DSS

(B). ISO 22301
(C). ISO 27001
(D). NIST CSF
Answer: A
Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirementsthat help prevent fraud

NO.483 An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?
(A). Order of volatility
(B). Data recovery
(C). Chain of custody
(D). Non-repudiation
Answer: C

NO.484 A company is implementing MFA for all applications that store sensitive dat a. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?
(A). One-time passwords
(B). Email tokens
(C). Push notifications
(D). Hardware authentication
Answer: C

NO.485 A security Daalyst is taking part in an evaluation process that analyzes and categorizes threat actors of real-world events in order to improve the incident response team's process.
Which of the following is the analyst MOST likely participating in?
(A). MITRE ATT&CK
B Walk-through
(B). Red team
(C). Purple team
(D). TAXII
Answer: B

NO.486 An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?
(A). HSM
(B). CASB
(C). TPM
(D). DLP
Answer: A

NO.487 A COMPANY HAS DESCOVERED UNA mans DEVICE ARE USING ITS WIFI NETWORK, AND IT

WANTS TO HARDEN THE ACCESS POINT TO IMPROVE SECURITY WHICH OF THE FOLLOWING CONFIGURATIONS SHOULD AN ANALYST ENABLE TO EMPROVE SECURITY? (SELECT TWO)
(A). RADIUS
(B). PEAP
(C). WPS
(D). WEP-TKIP
(E). SSL
(F). WPA2-PSK
Answer: D,F

AF

NO.488 A cybersecunty administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO)
(A). HIDS
(B). NIPS
(C). HSM
(D). WAF
(E). HIPS
(F). NIDS
(G). Stateless firewall
Answer: B,D

NO.489 A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?
(A). Shadow IT
(B). Credential stuffing
(C). SQL injection
(D). Man in the browser
(E). Bluejacking
Answer: A

NO.490 A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```


Which of the following is the security analyst observing?
(A). A rainbow table attack
(B). A password-spraying attack
(C). A dictionary attack
(D). A keylogger attack
Answer: C

NO.491 A SECURITY ANALYST NEEDS TO FIND REAL-TIME DATA ON THE LATEST MALWARE AND IoCs

WHICH OF THE FOLLOWING BEST DESCRIBE THE SOLUTION THE ANALYST SHOULD PERSUE?
(A). ADVISORIES AND BULLETINS
(B). THREAT FEEDS
(C). SECURITY NEWS ARTICLES
(D). PEER-REVIEWED CONTENT
Answer: B

NO.492 A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?
(A). Set up an air gap for the switch.
(B). Change the default password for the switch.
(C). Place the switch In a Faraday cage.
(D). Install a cable lock on the switch
Answer: B

NO.493 Local guidelines require that all information systems meet a minimum-security baseline to be compliant.
Which of the following can security administrators use to assess their system configurations against the baseline?
(A). SOAR playbook
(B). Security control matrix
(C). Risk management framework
(D). Benchmarks
Answer: D

NO.494 A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).
(A). Create a new network for the mobile devices and block the communication to the internal network and servers
(B). Use a captive portal for user authentication.
(C). Authenticate users using OAuth for more resiliency
(D). Implement SSO and allow communication to the internal network
(E). Use the existing network and allow communication to the internal network and servers.
(F). Use a new and updated RADIUS server to maintain the best solution
Answer: B,C

NO.495 Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?
(A). Privileged access management
(B). SSO

(C). RADIUS
(D). Attribute-based access control
Answer: A

NO.496 A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?
(A). MAC address filtering
(B). 802.1X
(C). Captive portal
(D). WPS
Answer: D

NO.497 An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?
(A). SOAP
(B). SAML
(C). SSO
(D). Kerberos
Answer: C

NO.498 Which biometric error would allow an unauthorized user to access a system?
(A). False acceptance
(B). False entrance
(C). False rejection
(D). False denial
Answer: C A

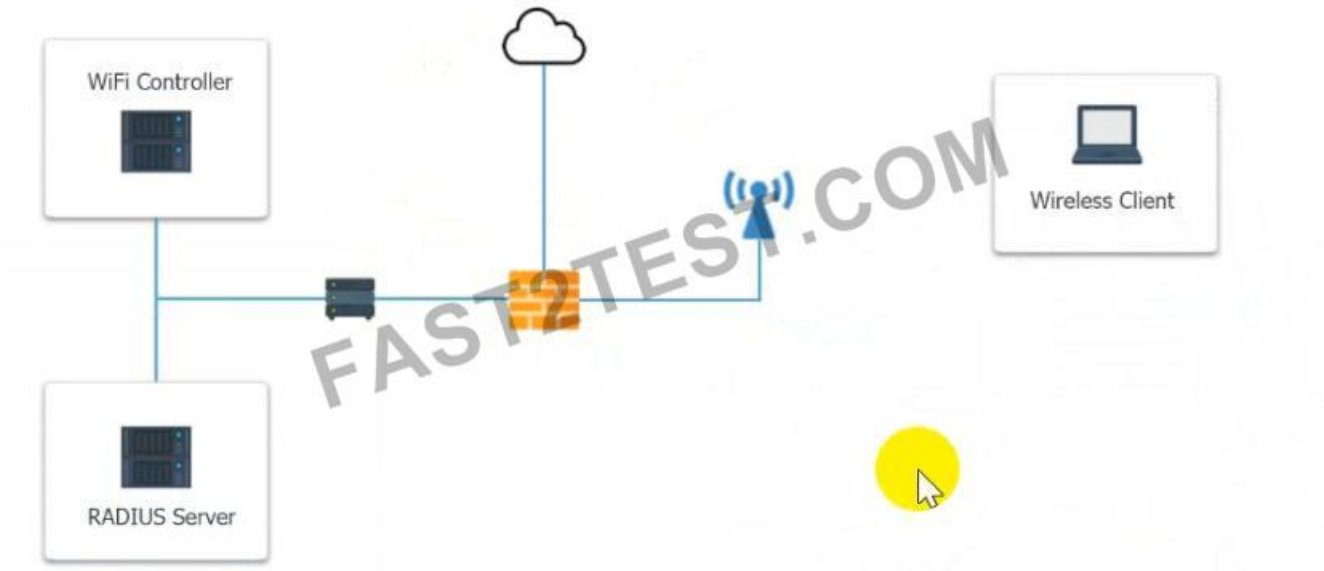
NO.499 When planning to build a virtual environment, an administrator need to achieve the following,
* Establish polices in Limit who can create new VMs
* Allocate resources according to actual utilization'
* Require justification for requests outside of the standard requirements.
* Create standardized categories based on size and resource requirements Which of the following is the administrator MOST likely trying to do?
(A). Implement IaaS replication
(B). Product against VM escape
(C). Deploy a PaaS
(D). Avoid VM sprawl
Answer: D

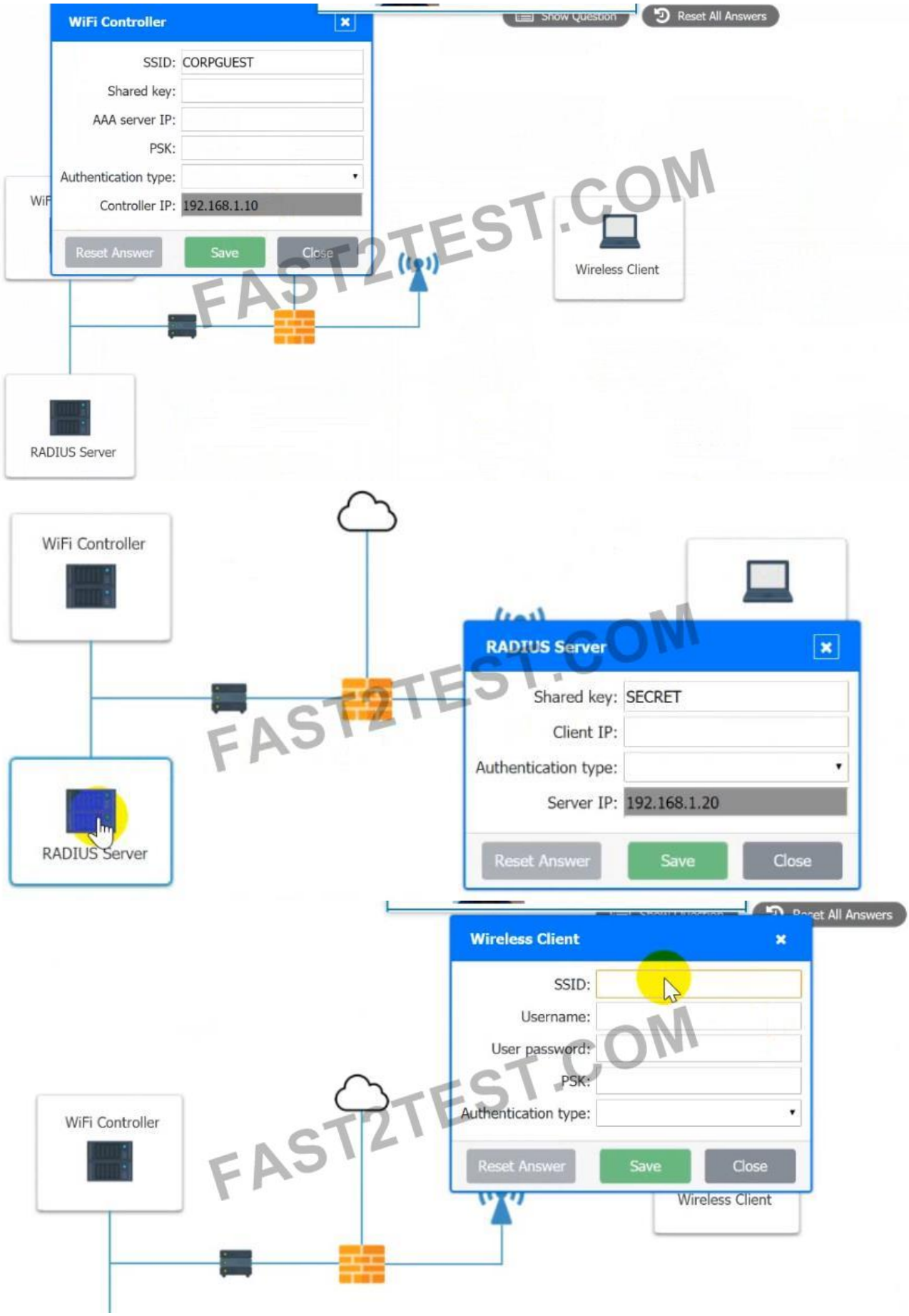
NO.500 During an incident a company CIRT determine it is necessary to observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

(A). Physical move the PC to a separate internet pint of presence
(B). Create and apply microsegmantion rules.
(C). Emulate the malware in a heavily monitored DM Z segment.
(D). Apply network blacklisting rules for the adversary domain
Answer: B

NO.501 Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time?
(A). PoC
(B). Production
(C). Test
(D). Development
Answer: A

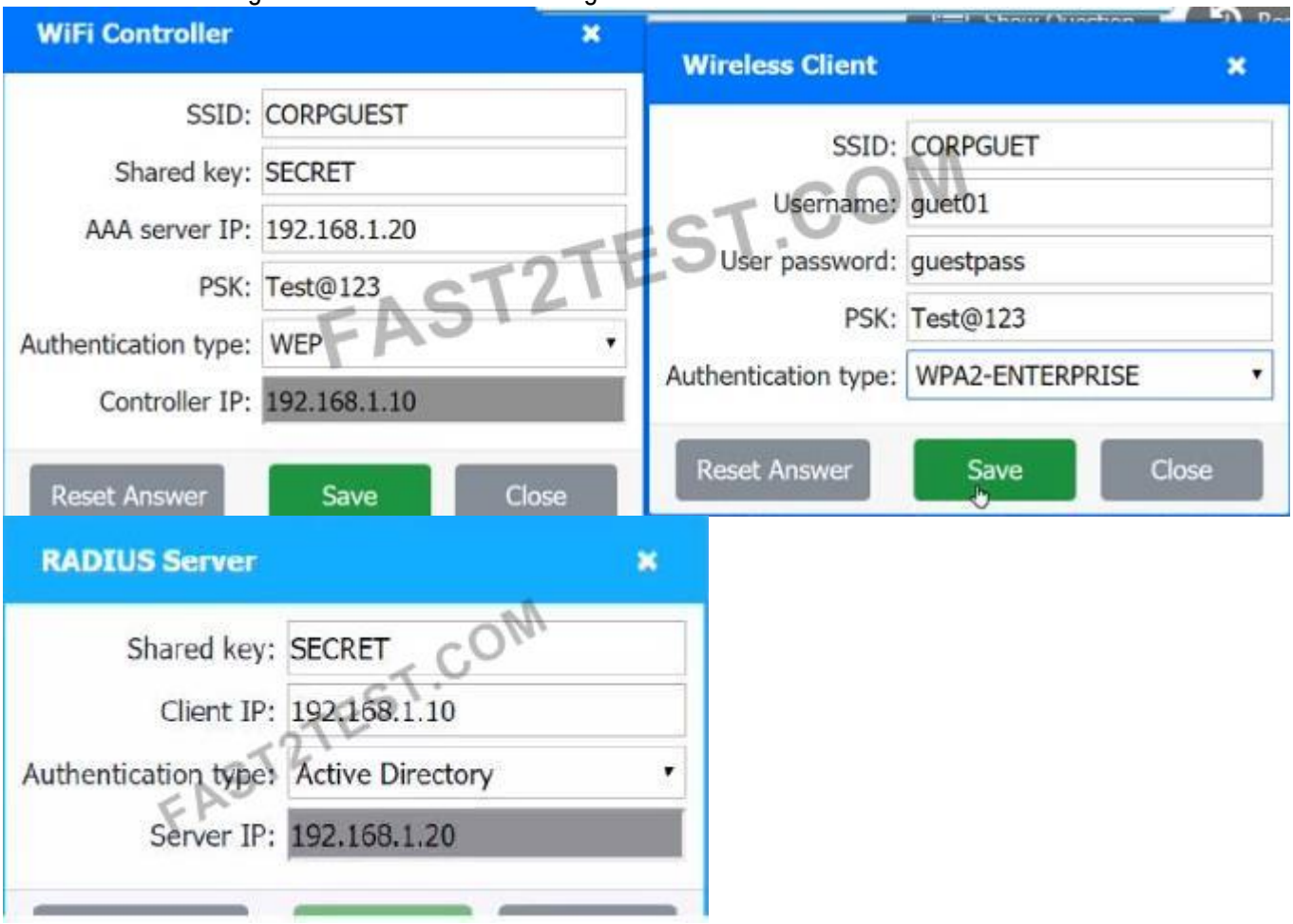
NO.502 A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.
Perform the following steps:
1. Configure the RADIUS server.
2. Configure the WiFi controller.
3. Preconfigure the client for an incoming guest. The guest AD credentials are:
User: guest01
Password: guestpass




Reset All Answers
WiFi Controller
SSID: CORPGUEST
Shared key:
AAA server IP:
PSK:
Authentication type:
Controller IP: 192.168.1.10
Reset Answer
Save
Close
Wireless Client
RADIUS Server
WiFi Controller
RADIUS Server
RADIUS Server
Shared key: SECRET
Client IP:
Authentication type:
Server IP: 192.168.1.20
Reset Answer
Save
Close
Reset All Answers
Wireless Client
SSID:
Username:
User password:
PSK:
Authentication type:
Reset Answer
Save
Close
WiFi Controller
Wireless Client
FAST2TEST.COM

Answer:

Use the same settings as describe in below images.



NO.503 During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:

Account	Login location	Time (UTC)	Message
user	New York	9:00 a.m.	Login: user, successful
user	Los Angeles	9:01 a.m.	Login: user, successful
user	Sao Paolo	9:05 a.m.	Login: user, successful
user	Munich	9:12 a.m.	Login: user, successful

Which Of the following account policies would BEST prevent attackers from logging in as user?
(A). Impossible travel time
(B). Geofencing
(C). Time-based logins
(D). Geolocation
Answer: A

NO.504 A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a

threat against the organization's network.
Which of the following will the analyst MOST likely use to accomplish the objective?
(A). A table exercise
(B). NST CSF
(C). MTRE ATT$CK
(D). OWASP
Answer: A C

NO.505 A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?
(A). Eradication
(B). Recovery
(C). Identification
(D). Preparation
Answer: C

NO.506 Which of the following would be indicative of a hidden audio file found inside of a piece of source code?
(A). Steganography
(B). Homomotphic encryption
(C). Cipher surte
(D). Blockchain
Answer: A
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

NO.507 An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate datacenter that houses confidential information There is a firewall at the Internet border followed by a DIP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?
(A). The DLP appliance should be integrated into a NGFW.
(B). Split-tunnel connections can negatively impact the DLP appliance's performance
(C). Encrypted VPN traffic will not be inspected when entering or leaving the network
(D). Adding two hops in the VPN tunnel may slow down remote connections
Answer: C

NO.508 An organization is planning to roll out a new mobile device policy and issue each employee a new laptop, These laptops would access the users' corporate operating system remotely and allow them to use the laptops for purposes outside of their job roles. Which of the following deployment models is being utilized?
(A). MDM and application management
(B). BYOO and containers
(C). COPE and VDI

(D). CYOD and VMs
Answer: C

NO.509 A technician enables full disk encryption on a laptop that will be taken on a business tnp. Which of the following does this process BEST protect?
(A). Data in transit
(B). Data in processing
(C). Data at rest
(D). Data tokenization
Answer: C
Data at rest: Data at rest is data in its stored or resting state, which is typically on some type of persistent storage such as a hard drive or tape. Symmetric encryption is used in this case.

NO.510 Which of the following are the BEST ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option? (Select Two)
(A). Install VPN concentrations at home offices
(B). Create NAT on the firewall for intranet systems
(C). Establish SSH access to a jump server
(D). Implement a SSO solution
(E). Enable MFA for intranet systems
(F). Configure SNMPv3 server and clients.
Answer: A,E

NO.511 A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?
(A). Implementation of preventive controls
(B). Implementation of detective controls
(C). Implementation of deterrent controls
(D). Implementation of corrective controls
Answer: B

NO.512 Interiprsing a secure area requires passing though two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?
(A). Cameras
B: Faraday cage
(B). Access control vestibule
(C). Sensors
(D). Guards
Answer: B

NO.513 A web server has been compromised due to a ransomware attack. Further investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

(A). The last incremental backup that was conducted 72 hours ago Most Voted
(B). The last known-good configuration Most Voted
(C). The last full backup that was conducted seven days ago
(D). The baseline OS configuration
Answer: C

A

Ransomware will most likely render the web server unusable and must be isolated for forensic investigation. This will leave the only option to start a new web server from scratch and restore the last full backup, plus any differential or incremental backups which are sure to be clean from ransomware (if available).

NO.514 A company recenty experienced an attack during which its main website was Girected to the attacker's web server, allowing the attacker to harvest credentials trom unsuspecting customers, Which of the following should the company implement lo prevent this type of attack from occurring In the future?
(A). PSec
(B). SSL/TLS
(C). ONSSEC
(D). SMIME
Answer: B

C

NO.515 Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?
(A). Data encryption
(B). Data masking
(C). Anonymization
(D). Tokenization
Answer: A

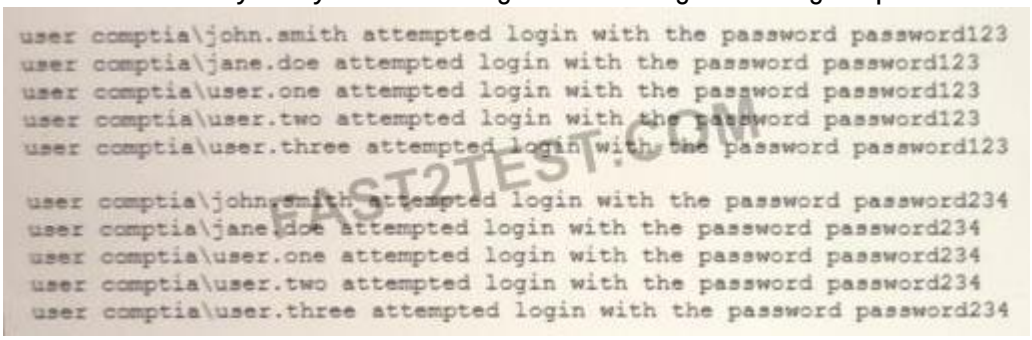
NO.516 A company wants the ability to restrict web access and monitor the websites that employees visit. Which of the following would BEST meet these requirements?
(A). internet proxy
(B). VPN
(C). WAF
(D). Firewall
Answer: C

A

NO.517 An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?
(A). Application allow list
(B). SWG
(C). Host-based firewall
(D). VPN
Answer: B

NO.518 A security manager runs Nessus scans of the network after every maintenance vandow Which of the following ts the securty manager MOST likely trying to accomplish?
(A). A Verifying that system patching has effectively removed known vulnerabilities
(B). identifying assets on the network that may not exist on the network asset inventory
(C). Validating the hosts do not have vulnerable ports exposed to the Intemet
(D). Checking the status of the automated malware analyses that is beang performed
Answer: A

NO.519 A security analyst is reviewing the following attack log output:



Which of the following types of attacks does this MOST likely represent?
(A). Rainbow table
(B). Brute-force
(C). Password-spraying
(D). Dictionary
Answer: C
Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.
https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:text=Password%20spraying%20is%20a%20type,rapid%20or%20frequent%20account%20lockouts.

NO.520 An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?
(A). Document the collection and require a sign-off when possession changes.
(B). Lock the device in a safe or other secure location to prevent theft or alteration.
(C). Place the device in a Faraday cage to prevent corruption of the data.
(D). Record the collection in a blockchain-protected public ledger
Answer: A

NO.521 During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?
(A). User behavior analytics
(B). Dump files
(C). Bandwidth monitors

(D). Protocol analyzer output
Answer: A

NO.522 The Chief Information Security Officer (CISO) of a bank recently updated the incident response policy. The CISO is concerned that members of the incident response team do not understand their roles. The bank wants to test the policy but with the least amount of resources or impact. Which of the following BEST meets the requirements?
(A). Warm site failover
(B). Tabletop walk-through
(C). Parallel path testing
(D). Full outage simulation
Answer: B

NO.523 Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?
(A). Rainbow table
(B). Dictionary
(C). Password spraying
(D). Pass-the-hash
Answer: C

NO.524 Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).
(A). Mantraps
(B). Security guards
(C). Video surveillance
(D). Fences
(E). Bollards
(F). Antivirus
Answer: A,B

BD

NO.525 A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?
(A). S/MIME
(B). LDAPS
(C). SSH
(D). SRTP

Answer: B

C

NO.526 Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).
(A). Page files
(B). Event logs
(C). RAM
(D). Cache
(E). Stored files
(F). HDD
Answer: A,D

CD

NO.527 When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?
(A). Z-Wave compatibility
(B). Network range
(C). Zigbee configuration
(D). Communication protocols
Answer: D

NO.528 A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?
(A). IaC
(B). MSSP
(C). Containers
(D). SaaS
Answer: A

NO.529 Aweb server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?
(A). NIC teaming
(B). High availability
(C). Dual power supply
(D). IaaS
Answer: B

NO.530 The Chief Information Security Officer directed a nsk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?
(A). CASB
(B). VPN concentrator
(C). MFA
(D). VPC endpoint
Answer: A

NO.531 An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?
(A). The system was configured with weak default security settings.
(B). The device uses weak encryption ciphers.
(C). The vendor has not supplied a patch for the appliance.
(D). The appliance requires administrative credentials for the assessment
Answer: C

NO.532 Which of the following involves the inclusion of code in the main codebase as soon as it is written?
(A). Continuous monitoring
(B). Continuous deployment
(C). Continuous Validation
(D). Continuous integration
Answer: D

* **NO.533** A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?
(A). Non-credentialed
(B). Web application
(C). Privileged
(D). Internal
Answer: B

A

NO.534 Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:
* All users share workstations throughout the day.
* Endpoint protection was disabled on several workstations throughout the network.
* Travel times on logins from the affected users are impossible.
* Sensitive data is being uploaded to external sites.
* All user account passwords were forced to be reset and the issue continued.
Which of the following attacks is being used to compromise the user accounts?
(A). Brute-force
(B). Keylogger
(C). Dictionary
(D). Rainbow
Answer: B

NO.535 Against the recommendation of the IT security analyst, a company set all user passwords on a server as "P@)55wOrD". Upon review of the /etc/passwa file, an attacker found the following:

hich of the following BEST explains why the encrypted passwords do not match?
(A). Perfect forward secrecy
(B). Key stretching
(C). Salting
(D). Hashing
Answer: C

NO.536 A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, ''Special privileges assigned to new login.'' Several of these messages did not have a valid logon associated with the user before these privileges were assigned.
Which of the following attacks is MOST likely being detected?
(A). Pass-the-hash
(B). Buffer overflow
(C). Cross-site scripting
(D). Session replay
Answer: A

NO.537 A company ts required to continue using legacy softveare to support a critical serwce.
Whech of the folowing BEST explans a reek of this prachce?
(A). Default system configuraton
(B). Unsecure protocols
(C). Lack of vendor support
(D). Weak encryption
Answer: B

NO.538 The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?
(A). Limit the use of third-party libraries.
(B). Prevent data exposure queries.
(C). Obfuscate the source code.
(D). Submit the application to QA before releasing it.
Answer: D

NO.539 An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?
(A). Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
(B). Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.

(C). incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
(D). Full backups Monday through Friday at 6:00 p.m and differential backups hourly.
Answer: A

NO.540 A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?
(A). Due to foreign travel, the user's laptop was isolated from the network.
(B). The user's laptop was quarantined because it missed the latest path update.
(C). The VPN client was blacklisted.
(D). The user's account was put on a legal hold
Answer: A

NO.541 Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?
(A). The data owner
(B). The data processor
(C). The data steward
(D). The data privacy officer.
Answer: C

NO.542 A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?
(A). SQLi
(B). CSRF
(C). Session replay
(D). API
Answer: C

B

NO.543 Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?
(A). Standard naming conventions
(B). Domain services
(C). Baseline configurations
(D). Diagrams
Answer: C

A

NO.544 An organization is having difficulty correlating events from its individual AV, EDR. DLP. SWG, WAF, MDM. HIPS. and CASB systems. Which of the following Is the BEST way to improve the

situation?
(A). Remove expensive systems that generate few alerts,
(B). Modify the systems to alert only on critical issues.
(C). Utilize a SIEM to centralize logs and dashboards.
(D). implement a new syslog/NetFlow appliance.
Answer: B

C

NO.545 Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?
(A). GDPR
(B). PCI DSS
(C). ISO 27000
(D). NIST 800-53
Answer: D

NO.546 DDoS attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfils the architect's requirements?
(A). An orchestration solution that can adjust scalability of cloud assets
(B). Use of multipath by adding more connections to cloud storage
(C). Cloud assets replicated on geographically distributed regions
(D). An on-site backup that is deployed and only used when the load increases
Answer: A
Scaling cloud infrastructures can experience lag during the periods of high activity, where other assets have to either be added, or become active. This is the compromise for a cost-effective solution that scales. The company could go for a system that is absolutely overkill on assets at all times, in preparation for those brief peak moments. But this is expensive, and unlikely to be taken by most companies. Only case you would want to use one of these is if you have a sensitive or critical service that MUST remain online. Stock exchange servers, military servers, bank servers, etc. come to mind for this criteria.

NO.547 Several attempts have been made lo pick the door lock of a secure facility As a result the security engineer has been assigned to implement a stronger preventative access control Which of the following would BEST complete 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
Answer: D

A

NO.548 The website http://companywebsite.com requires users to provide personal information including security responses, for registration. which of the following would MOST likely cause a date breach?
(A). LACK OF INPUT VALIDATION
(B). OPEN PERMISSIONS
(C). UNSCECURE PROTOCOL

(D). MISSING PATCHES
Answer: A

C

NO.549 A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following
* The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
* One of the websites the manager used recently experienced a data breach
* The manager's corporate email account was successfully accessed in the last fve days by an IP address located in a foreign country Which of the following attacks has MOST hkely been used to compromise the manager's corporate account?
(A). Remote access Trojan
(B). Brute-force
(C). Oicbonary
(D). Credential stuffing
(E). Password spraying
Answer: D

NO.550 Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?
(A). An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
(B). An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
(C). Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
(D). Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites
Answer: A

D

NO.551 Which of the following terms describes a broad range of information that is sensitive to a specific organization?
(A). Public
(B). Top secret
(C). Proprietary
(D). Open-source
Answer: C

NO.552 A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?
(A). Preventive
(B). Compensating
(C). Corrective
(D). Detective
Answer: D

NO.553 A security analyst receives an alert from trie company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192 168.3426. Which of the following describes this type of alert?
(A). True positive
(B). True negative
(C). False positive
(D). False negative
Answer: C

NO.554 While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?
(A). SNMP traps
(B). A Telnet session
(C). An SSH connection
(D). SFTP traffic
Answer: B

NO.555 A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?
(A). Nmap
(B). Wireshark
(C). Autopsy
(D). DNSEnum
Answer: A

NO.556 A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?
(A). A new firewal rule is needed to access the application.
(B). The system was quarantined for missing software updates.
(C). The software was not added to the application whitelist.
(D). The system was isolated from the network due to infected software
Answer: C

NO.557 As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?
(A). User behavior analysis
(B). Packet captures
(C). Configuration reviews
(D). Log analysis
Answer: D
A vulnerability scanner is essentially doing that. It scans every part of your network configuration that it can, and determines if known vulnerabilities are known at any point of that.

NO.558 A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?
(A). Fileless malware
(B). A downgrade attack
(C). A supply-chain attack
(D). A logic bomb
(E). Misconfigured BIOS
Answer: C

NO.559 An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

Which of the following is the MOST likely cause of the issue?
(A). The end user purchased and installed a PUP from a web browser
(B). A bot on the computer is brute forcing passwords against a website
(C). A hacker is attempting to exfiltrate sensitive data
(D). Ransomware is communicating with a command-and-control server
Answer: A

NO.560 Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process ?
(A). Data breach notification
(B). Accountability
(C). Legal hald
(D). Chain of custody
Answer: C

NO.561 A recent audit cited a risk involving numerous low-criticality vulnerabilities created by a web application using a third-party library. The development staff state there are still customers using the application even though it is end of life and it would be a substantial burden to update the application for compatibility with more secure libraries. Which of the following would be the MOST prudent course of action?
(A). Accept the risk if there is a clear road map for timely decommission
(B). Deny the risk due to the end-of-life status of the application.

(C). Use containerization to segment the application from other applications to eliminate the risk
(D). Outsource the application to a third-party developer group
Answer: C

NO.562 Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)
(A). Unsecure protocols
(B). Use of penetration-testing utilities
(C). Weak passwords
(D). Included third-party libraries
(E). Vendors/supply chain
(F). Outdated anti-malware software
Answer: A,D DE

NO.563 A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describes these systems?
(A). DNS sinkholes
(B). Hafieypots
(C). Virtual machines
(D). Neural networks
Answer: B

NO.564 Which of the following types of controls is a CCTV camera that is not being monitored?
(A). Detective
(B). Deterrent
(C). Physical
(D). Preventive
Answer: B

NO.565 A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees. Which of the following controls.
should the company consider using as part of its IAM strategy? (Select TWO).
(A). A complex password policy
(B). Geolocation
(C). An impossible travel policy
(D). Self-service password reset
(E). Geofencing
Answer: A,B
F Time-based logins

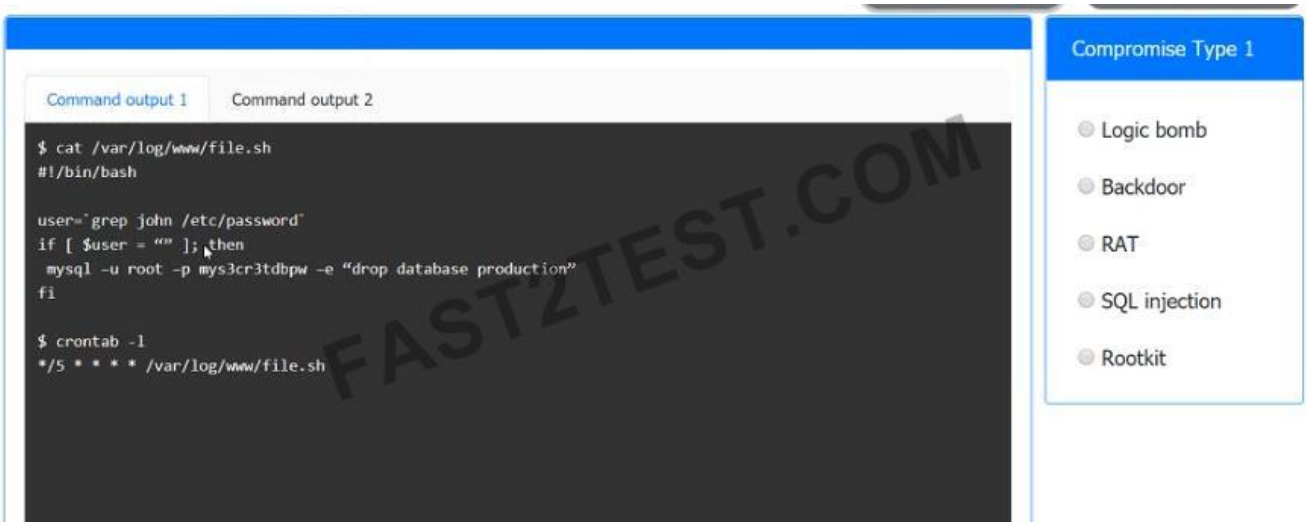
NO.566 The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

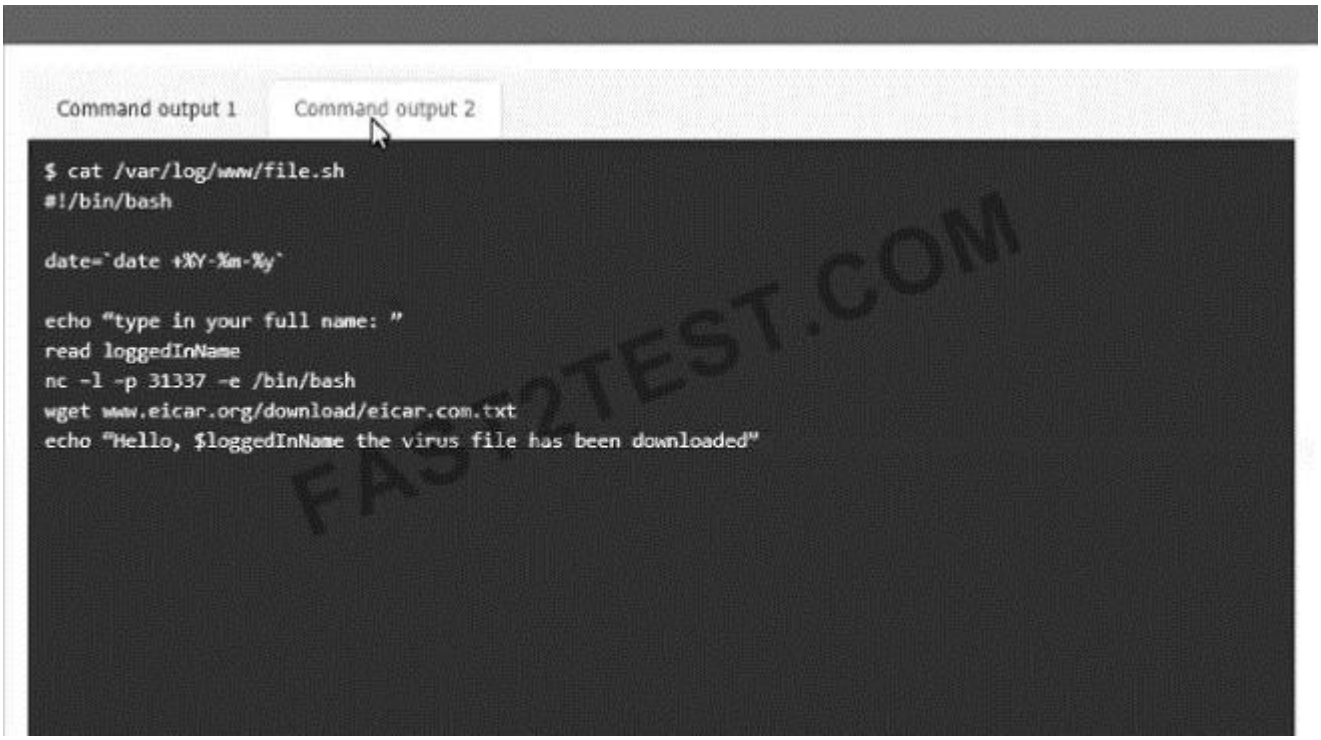
(A). Phishing
(B). Whaling
(C). Type squatting
(D). Pharming
Answer: B

NO.567 Which of the following statements BEST describes zero-day exploits'?
(A). When a zero-day exploit is discovered, the system cannot be protected by any means
(B). Zero-day exploits have their own scoring category in CVSS
(C). A zero-day exploit is initially undetectable and no patch for it exists
(D). Discovering zero-day exploits is always performed via bug bounty programs
Answer: C

NO.568 An analyst is trying to identify insecure services thal are running on the intemal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)
(A). SFTP. FIPS
(B). SNMPv2, SNMPv3
(C). HTTP, HTTPS
D TFTP, FTP
(D). SNMPyt, SNMPy2
(E). Tenet, SSH
(F). TLS, SSL
(G). POP, IMAP
(H). Login, nogin
Answer: A,D,F BCE

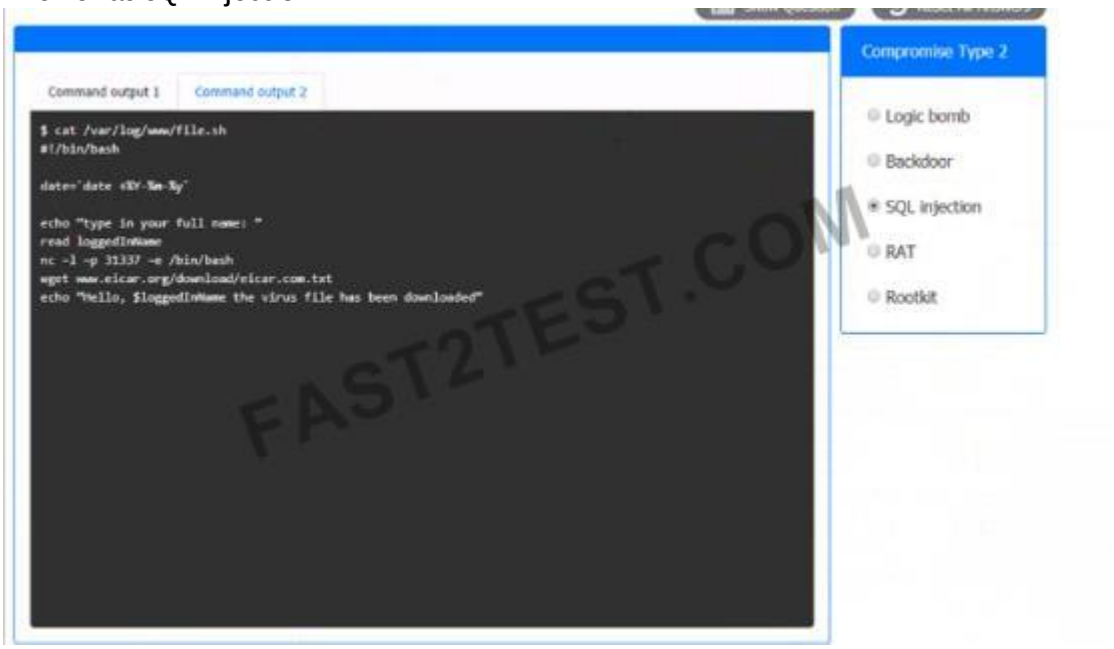
NO.569 An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

Answer as SQL injection



NO.570 During a security incident investigation, an analyst consults the company's SIEM and sees an event concerning high traffic to a known, malicious command-and-control server. The analyst would like to determine the number of company workstations that may be impacted by this issue. Which of the following can provide the information?

(A). WAF logs

(B). DNS logs

(C). System logs

(D). Application logs

Answer: B

NO.571 A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).
(A). 135
(B). 139
(C). 143
(D). 161
(E). 443
(F). 445
Answer: A,E

BF

NO.572 A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?
(A). Checksums
(B). Watermarks
(C). Oder of volatility
(D). A log analysis
(E). A right-to-audit clause
Answer: D
https://www.sumologic.com/glossary/log-analysis/
"While companies can operate private clouds, forensics in a public cloud are complicated by the right to audit permitted to you by your service level agreement (SLA) with the cloud provider."

NO.573 An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?
(A). PEAP
(B). EAP-FAST
(C). EAP-TLS
(D). EAP-TTLS
Answer: C

A

NO.574 Which of the following should a data owner require all personnel to sign to legally protect intellectual property?
(A). An NDA
(B). An AUP
(C). An ISA
(D). An MOU
Answer: D

A

NO.575 A smail business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the

business network. Which of the following would BEST support the office's business needs? (Select TWO)
(A). Installing WAPs with strategic placement
(B). Configuring access using WPA3
(C). Installing a WIDS
(D). Enabling MAC filtering
(E). Changing the WiFi password every 30 days
(F). Reducing WiFi transmit power throughout the office
Answer: B,D

NO.576 An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?
(A). Shadow IT
(B). An insider threat
(C). A hacktivist
(D). An advanced persistent threat
Answer: D
https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
https://csrc.nist.gov/glossary/term/advanced_persistent_threat

NO.577 An organization is concerned that is hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?
(A). Hping3 -s comptia, org -p 80
(B). Nc -1 -v comptia, org -p 80
(C). nmp comptia, org -p 80 -aV
(D). nslookup -port=80 comtia.org
Answer: C
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

NO.578 After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).
(A). Disabling guest accounts
(B). Disabling service accounts
(C). Enabling network sharing
(D). Disabling NetBIOS over TCP/IP
(E). Storing LAN manager hash values
(F). Enabling NTLM
Answer: A,D

NO.579 A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?
(A). The scan results show open ports, protocols, and services exposed on the target host

(B). The scan enumerated software versions of installed programs
(C). The scan produced a list of vulnerabilities on the target host
(D). The scan identified expired SSL certificates
Answer: B

NO.580 A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?
(A). Geotargeting
(B). Geolocation
(C). Geotagging
(D). Geofencing

Answer: B

D

NO.581 After a recent security breach, a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?
(A). SSH
(B). SNMPv3
(C). SFTP
(D). Telnet
(E). FTP
Answer: A

NO.582 A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

```
http://company.com/../../../etc/passwd
```

Which ol the following types of attacks is being attempted and how can it be mitigated?
(A). XSS. mplement a SIEM
(B). CSRF. implement an IPS
(C). Directory traversal implement a WAF
(D). SQL infection, mplement an IDS
Answer: C

NO.583 Which of the following would satisfy three-factor authentication?
(A). Password, retina scanner, and NFC card
(B). Password, fingerprint scanner, and retina scanner
(C). Password, hard token, and NFC card
(D). Fingerpnint scanner, hard token, and retina scanner
Answer: C

A

NO.584 An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

```
Session          : hashcat
Status           : cracked
Hash.Type        : MD5
Hash.Target      : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started     : Fri Mar 10 10:18:45 2020
Recovered        : 1/1 (100%) Digests
Progress         : 28756845 / 450365879 (6.38%) hashes
Time.Stopped     : Fri Mar 10 10:20:12 2020
Password found   : Th3B3stP@55w0rd!
```


Which of the following BEST describes the type of password attack the attacker is performing?
(A). Dictionary
(B). Pass-the-hash
(C). Brute-force
(D). Password spraying
Answer: A

NO.585 A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and Is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?
(A). Dual power supplies
(B). AUPS
(C). A generator
(D). APDU
Answer: B

NO.586 An organization Chief information Security Officer a position that will be responsibles for implementing technical controls to protect data, include ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?
(A). Data protection officer
(B). Data owner
(C). Backup administrator
(D). Data custodian
(E). Internal auditor
Answer: A

D

NO.587 Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?
(A). A right-to-audit clause allowing for annual security audits
(B). Requirements for event logs to be kept for a minimum of 30 days
(C). Integration of threat intelligence in the company's AV
(D). A data-breach clause requiring disclosure of significant data loss
Answer: A

NO.588 Which of the following algorithms has the SMALLEST key size?

(A). DES
(B). Twofish
(C). RSA
(D). AES
Answer: B

NO.589 uring an investigation, a security manager receives notification from local authorities that company proprietary data was found on a former employee's home computer. The former employee's corporate workstation has since been repurposed, and the data on the hard drive has been overwritten. Which of the following would BEST provide the security manager with enough details to determine when the data was removed from the company network?
(A). Properly configured hosts with security logging
(B). Properly configured endpoint security tool with alerting
(C). Properly configured SIEM with retention policies
(D). Properly configured USB blocker with encryption
Answer: C

A

NO.590 A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?
(A). Configure the perimeter firewall to deny inbound external connections to SMB ports.
(B). Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
(C). Deny unauthenticated users access to shared network folders.
(D). Verify computers are set to install monthly operating system, updates automatically.
Answer: A

NO.591 The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer dat a. Which of the following would be BEST for the third-party vendor to provide to the CISO?
(A). GDPR compliance attestation
(B). Cloud Security Alliance materials
(C). SOC 2 Type 2 report
(D). NIST RMF workbooks
Answer: C
https://www.itgovernance.co.uk/soc-reporting

NO.592 Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?
(A). An SLA
(B). AnNDA
(C). ABPA
(D). AnMOU
Answer: D

NO.593 Which of the following should an organization consider implementing In the event

executives need to speak to the media after a publicized data breach?
(A). Incident response plan
(B). Business continuity plan
(C). Communication plan
(D). Disaster recovery plan
Answer: D

C

NO.594 Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?
(A). Risk matrix
(B). Risk tolerance
(C). Risk register
(D). Risk appetite
Answer: D

B

NO.595 A systoms administrator needs to instal the seme X.509 certificate on multiple servers. Which of the following should the administrator use?
(A). Key escrow
(B). Asself-signed certificate
(C). Cerificate chaining
(D). An extended validation certificate
Answer: B

NO.596 A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:
www.company.com (main website)
contactus.company.com (for locating a nearby location)
quotes.company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?
(A). SAN
(B). Wildcard
(C). Extended validation
(D). Self-signed
Answer: B

NO.597 A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?
(A). A non-disclosure agreement
(B). Least privilege
(C). An acceptable use policy
(D). Ofboarding
Answer: D

NO.598 A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?
(A). Time-based logins
(B). Geofencing
(C). Network location
(D). Password history
Answer: A

NO.599 A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation, Which of the following would dispute the analyst's claim of innocence?
(A). Legal hold
(B). Order of volatility
(C). Non-repudiation
(D). Chain of custody
Answer: D

C

NO.600 nteping a secure area requires passing though two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?
(A). Cameras
B: Faraday cage
(B). Access control vestibule
(C). Sensors
(D). Guards
Answer: B

NO.601 An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?
(A). Jamming
(B). Bluesnarfing
(C). Evil twin
(D). Rogue access point
Answer: D

NO.602 A security manager has tasked the security operations center with locating all web servers that respond to an unsecure protocol. Which of the following commands could an analyst run to find requested servers?
(A). nslookup 10.10.10.0
(B). nmap -p 80 10.10.10.0/24
(C). pathping 10.10.10.0 -p 80
(D). no -1 -p 80
Answer: B

NO.603 Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?
(A). Footprinting
(B). White-box testing
(C). A drone/UAV
(D). Pivoting
Answer: A

NO.604 An organization has implemented a two-step verification process to protect user access to data that s stored in the coud lc scssnncsitcibin a vdiemiietanebins code to access the dat a. Which of the following authentication methods did the organization implement?
(A). Token key
(B). B Static code
(C). Push notification
Answer: A
'D. HOTP
D

NO.605 An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:
(A). business continuity plan
(B). communications plan.
(C). disaster recovery plan.
(D). continuity of operations plan
Answer: C

NO.606 A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO from sending email from a work account to a personal account. Which of the following types of service providers is being used?
(A). Telecommunications service provider
(B). Cloud service provider
(C). Master managed service provider
(D). Managed security service provider
Answer: B

NO.607 A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?
(A). AH
(B). ESP
(C). SRTP
(D). LDAP
Answer: B
A

NO.608 A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

(A). Unsecme protocols
(B). Default settings
(C). Open permissions
(D). Weak encryption
Answer: D

NO.609 An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organizations requirement?
(A). Perform OSINT investigations
(B). Subscribe to threat intelligence feeds
(C). Submit RFCs
(D). Implement a TAXII server
Answer: B D

NO.610 A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?
(A). Add a deny-all rule to that host in the network ACL
(B). Implement a network-wide scan for other instances of the malware.
(C). Quarantine the host from other parts of the network
(D). Revoke the client's network access certificates
Answer: C

B

NO.611 A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```


Which of the following is the router experiencing?
(A). DDoS attack
(B). Memory leak
(C). Buffer overflow
(D). Resource exhaustion
Answer: D

NO.612 A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?
(A). Key escrow
(B). A self-signed certificate
(C). Certificate chaining
(D). An extended validation certificate
Answer: C B

NO.613 A company's Chief Information Office (CIO) is meeting with the Chief Information Security

Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?
(A). A capture-the-flag competition
(B). A phishing simulation
(C). Physical security training
(D). Baste awareness training
Answer: B

A

NO.614 A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know was in the memory on the compromised server. Which of the following files should be given to the forensics firm?
(A). Security
(B). Application
(C). Dump
(D). Syslog
Answer: C
Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them
https://www.digitalcitizen.life/view-contents-dump-file/

NO.615 Which of the following is the correct order of volatility from MOST to LEAST volatile? >
(A). Memory, temporary filesystems, routing tables, disk, network storage
(B). Cache, memory, temporary filesystems, disk, archival media
(C). Memory, disk, temporary filesystems, cache, archival media
(D). Cache, disk, temporary filesystems, network storage, archival media
Answer: B

NO.616 Which of the following refers to applications and systems that are used within an organization without consent or approval?
(A). Shadow IT
(B). OSINT
(C). Dark web
(D). Insider threats
Answer: A

NO.617 Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

```
Domain Name: COMPTIA.ORG
Registry Domain ID: 1234554321
Registrar Server: whois.networksolutions.com
Updated Date: 2018-12-01T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC
Registrar IANA ID: 2
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: YourBusiness Corporation
Registrant Organization: YourBusiness Corporation
Registrant Street: 500 Pennsylvania Ave
Registrant City: Downers Grove
Registrant State: IL
Registrant Postal Code: 11105
Registrant Country: US
Registrant Phone: 1 800 555 5555
Registrant Fax: 1 800 555 5556
Registrant Email: info@comptia.org
Admin:  Jason Doe
Admin Organization: CompTIA
```


Which of the following can be determined about the organization's public presence and security posture? (Select TWO).
(A). Joe used Whois to produce this output.
(B). Joe used cURL to produce this output.
(C). Joe used Wireshark to produce this output.
(D). The organization has adequate information available in public registration.
E: The organization has too much information available in public registration.
(E). The organization has too little information available in public registration.
Answer: A,D

NO.618 An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:
(A). MTBF
(B). RPO
(C). MTTR
(D). RTO
Answer: D
https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/

NO.619 Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?
(A). Data encryption
(B). Data masking
(C). Data deduplication
(D). Data minimization

Answer: B

NO.620 A systems administrators considering diferent backup solitons forthe IT rkashuchre The company 5 looky fre sokton tha ofes the fastest recovery ime whie aso saving the most amount of storage used to maintain the backups Which of the following recovery solubons would be the BEST option to meet these requirements?
(A). Snapshot
(B). Differentiated
(C). Full
(D). Tape
Answer: B

NO.621 The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?
(A). CASB
(B). Next-generation SWG
(C). NGFW
(D). Web-application firewall
Answer: B

NO.622 Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?
(A). Investigation
(B). Containment
(C). Recovery
(D). Lessons learned
Answer: B

NO.623 A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company's cloud environment Which of the following is an immediate consequence of these integrations?
(A). Non-compliance with data sovereignty rules
(B). Loss of the vendor's interoperability support
(C). Mandatory deployment of a SIEM solution
(D). Increase in the attack surface
Answer: A

D

NO.624 A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?
(A). Containment
(B). Identification
(C). Recovery

(D). Preparation
Answer: B

NO.625 Which of the following tools is effective in preventing a user from accessing unauthorized removable media?
(A). USB data blocker
(B). Faraday cage
(C). Proximity reader
(D). Cable lock
Answer: B
A

NO.626 Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log m to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)
(A). COPE
(B). VDI
(C). GPS
(D). TOTP
(E). RFID
(F). BYOD
Answer: B,E

NO.627 Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).
Testing security systems and processes regularly
(A). Installing and maintaining a web proxy to protect cardholder data
(B). Assigning a unique ID to each person with computer access
(C). Encrypting transmission of cardholder data across private networks
(D). Benchmarking security awareness training for contractors
(E). Using vendor-supplied default passwords for system passwords
Answer: B,D
test assign

NO.628 A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?
(A). Disable unneeded services.
(B). Install the latest security patches.
(C). Run a vulnerability scan.
(D). Encrypt all disks.
Answer: C

NO.629 The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?
(A). Preventing any current employees' siblings from working at the bank to prevent nepotism
(B). Hiring an employee who has been convicted of theft to adhere to industry compliance
(C). Filtenng applicants who have added false information to resumes so they appear better qualified

(D). Ensuring no new hires have worked at other banks that may be trying to steal customer information

Answer: B

NO.630 Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

(A). CVSS
(B). SIEM
(C). SOAR
(D). CVE

Answer: A

CVSS is maintained by the Forum of Incident Response and Security Teams (first.org/cvss). CVSS metrics generate a score from 0 to 10 based on characteristics of the vulnerability, such as whether it can be triggered remotely or needs local access, whether user intervention is required, and so on

NO.631 The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3$"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

(A). Password history
(B). Account expiration
(C). Password complexity
(D). Account lockout

Answer: D

NO.632 A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

(A). Establish chain of custody.
(B). Inspect the file metadata.
(C). Reference the data retention policy.
(D). Review the email event logs

Answer: D

NO.633 An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

(A). Data custodian
(B). Data controller
(C). Data proton officer
(D). Data processor

Answer: C

B

NO.634 Which of the following authentication methods is considered to be the LEAST secure?
(A). TOTP
(B). SMS
(C). HOTP
(D). Token key
Answer: B

NO.635 Which of the following is an example of transference of risk?
(A). Purchasing insurance
(B). Patching vulnerable servers
(C). Retiring outdated applications
(D). Application owner risk sign-off
Answer: A

NO.636 Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?
(A). Phishing
(B). Vishing
(C). Smishing
(D). Spam
Answer: C
Smishing is a type of phishing attack which begins with an attacker sending a text message to an individual. The message contains social engineering tactics to convince the person to click on a malicious link or send sensitive information to the attacker. Criminals use smishing attacks for purposes like:
Learn login credentials to accounts via credential phishing
Discover private data like social security numbers
Send money to the attacker
Install malware on a phone
Establish trust before using other forms of contact like phone calls or emails Attackers may pose as trusted sources like a government organization, a person you know, or your bank. And messages often come with manufactured urgency and time-sensitive threats. This can make it more difficult for a victim to notice a scam.
Phone numbers are easy to spoof with VoIP texting, where users can create a virtual number to send and receive texts. If a certain phone number is flagged for spam, criminals can simply recycle it and use a new one.

NO.637 A security analyst has been asked by the Chief Information Security Officer to
* develop a secure method of providing centralized management of infrastructure
* reduce the need to constantly replace aging end user machines
* provide a consistent user desktop expenence
Which of the following BEST meets these requirements?
(A). BYOD

(B). Mobile device management
(C). VDI
(D). Containers ation
Answer: C

NO.638 Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?
(A). Watering-hole attack
(B). Credential harvesting
(C). Hybrid warfare
(D). Pharming
Answer: A
An attack in which an attacker targets specific groups or organizations, discovers which websites they frequent, and injects malicious code into those sites.

NO.639 Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?
(A). DNSSEC and DMARC
(B). DNS query logging
(C). Exact mail exchanger records in the DNS
(D). The addition of DNS conditional forwarders
Answer: C

NO.640 The president of a regional bank likes to frequently provide SOC tours to potential investors. Which of the following policies BEST reduces the risk of malicious activity occurring after a tour?
(A). Password complexity
(B). Acceptable use
(C). Access control
(D). Clean desk
Answer: D

NO.641 A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?
(A). Use fuzzing testing
(B). Use a web vulnerability scanner
(C). Use static code analysis
(D). Use a penetration-testing OS
Answer: C

NO.642 A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?
(A). Vulnerability feeds

(B). Trusted automated exchange of indicator information
(C). Structured threat information expression
(D). Industry information-sharing and collaboration groups
Answer: D

NO.643 Which of the following ISO standards is certified for privacy?
(A). ISO 9001
(B). ISO 27002
(C). ISO 27701
(D). ISO 31000
Answer: C
ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems.
https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701

NO.644 Which of the following scenarios BEST describes a risk reduction technique?
(A). A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
(B). A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
(C). A security control objective cannot be met through a technical change, so the company changes as method of operation
(D). A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.
Answer: B

NO.645 A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?
(A). Create DLP controls that prevent documents from leaving the network
(B). Implement salting and hashing
(C). Configure the web content filter to block access to the forum.
(D). Increase password complexity requirements
Answer: A B

NO.646 A news article states that a popular web browser deployed on all corporate PCs is vulnerable to a zero-day attack. Which of the following MOST concerns the Chief Information Security Officer about the information in the news article?
(A). Insider threats have compromised this network.
(B). Web browsing is not functional for the entire network.
(C). Antivirus signatures are required to be updated immediately.
(D). No patches are available for the web browser.
Answer: D

NO.647 While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?
(A). A RAT was installed and is transferring additional exploit tools.
(B). The workstations are beaconing to a command-and-control server.
(C). A logic bomb was executed and is responsible for the data transfers.
(D). A fireless virus is spreading in the local network environment
Answer: A

NO.648 Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?
(A). Staging
(B). Test
(C). Production
(D). Development
Answer: B

A

NO.649 A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?
(A). HIDS
(B). UEBA
(C). CASB
(D). VPC
Answer: C

NO.650 Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?
(A). DDoS
(B). Man-in-the-middle
(C). MAC flooding
(D). Domain hijacking

Answer: A

NO.651 Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?
(A). DLP
(B). HIDS
(C). EDR
(D). NIPS

Answer: C

NO.652 A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?
(A). Implementation of corrective controls
(B). Implementation of preventive controls
(C). Implementation of deterrent controls
(D). Implementation of detective controls
Answer: D

NO.653 An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has not received information about the internal architecture. Which of the following BEST represents the type of testing that will occur?
(A). Gray-box
(B). White-box
(C). Bug bounty
(D). Black-box
Answer: D

NO.654 During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the nsk of lateral spread and the nsk that the adversary would notice any changes?
(A). Physically move the PC to a separate Internet point of presence.
(B). Create and apply microsegmentation rules,
(C). Emulate the malware in a heavily monitored DMZ segment
(D). Apply network blacklisting rules for the adversary domain
Answer: C

B

NO.655 A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?
(A). A captive portal
(B). PSK
(C). 802.1X
(D). WPS
Answer: C

NO.656 A network engineer at a company with a web server is building a new web environment with the following requirements:
* Only one web server at a time can service requests.
* If the primary web server fails, a failover needs to occur to ensure the secondary web server becomes the primary.
Which of the following load-balancing options BEST fits the requirements?
(A). Cookie-based
(B). Active-passive

(C). Persistence
(D). Round robin
Answer: A B

NO.657 Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?
(A). The data protection officer
(B). The data processor
(C). The data owner
(D). The data controller
Answer: C

NO.658 A Chief Information Security Officer has defined resiliency requirements for a new data center architecture The requirements are as follows
* Critical fileshares will remain accessible during and after a natural disaster
* Frve percent of hard disks can fail at any given time without impacting the data.
* Systems will be forced to shut down gracefully when battery levels are below 20% Which of the following are required to BEST meet these objectives? (Select THREE)
(A). Fiber switching
(B). IaC
(C). NAS
(D). RAID
(E). UPS
(F). Redundant power supplies
(G). Geographic dispersal
(H). Snapshots
(I). Load balancing
Answer: D,E,G

NO.659 A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

Which of the following can the security analyst conclude?
(A). A replay attack is being conducted against the application.
(B). An injection attack is being conducted against a user authentication system.
(C). A service account password may have been changed, resulting in continuous failed logins within the application.
(D). A credentialed vulnerability scanner attack is testing several CVEs against the application.
Answer: C

NO.660 A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security team has been instructed to resolve the problem as quickly as possible causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?
(A). Update the host firewalls to block outbound SMB.
(B). Place the machines with the unapproved software in containment.
(C). Place the unauthorized application in a blocklist.
(D). Implement a content filter to block the unauthorized software communication.
Answer: B

NO.661 A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?
(A). Enforce the use of a controlled trusted source of container images
(B). Deploy an IPS solution capable of detecting signatures of attacks targeting containers
(C). Define a vulnerability scan to assess container images before being introduced on the environment
(D). Create a dedicated VPC for the containerized environment
Answer: D

A

NO.662 Which of the following policies establishes rules to measure third-party work tasks and ensure deliverables are provided within a specific time line?
(A). SLA
(B). MOU
(C). AUP
(D). NDA
Answer: A

NO.663 A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?
(A). IP conflict
(B). Pass-the-hash
(C). MAC flooding
(D). Directory traversal

(E). ARP poisoning
Answer: E
https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning

NO.664 A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)
(A). Dual power supply
(B). Off-site backups
(C). Automatic OS upgrades
(D). NIC teaming
(E). Scheduled penetration testing
(F). Network-attached storage
Answer: A,B
https://searchdatacenter.techtarget.com/definition/resiliency

NO.665 Which of the following is the FIRST environment in which proper, secure coding should be practiced?
(A). Stage
(B). Development
(C). Production
(D). Test
Answer: B
The developer has to start writing secure code from beginning itself. Which will then be tested, staged and finally production

NO.666 Which of the technologies is used to actively monitor for specific file types being transmitted on the network?
(A). File integrity monitoring
(B). Honeynets
(C). Tcpreplay
(D). Data loss prevention
Answer: B

NO.667 An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?
(A). Delete the private key from the repository.
(B). Verify the public key is not exposed as well.
(C). Update the DLP solution to check for private keys.
(D). Revoke the code-signing certificate.
Answer: A D
We need to revoke the code-signing certificate as this is the most secure way to ensure that the comprised key wont be used by attackers. Usually there are bots crawking all over repos searching this kind of human errors.

NO.668 A security analyst reports a company policy volation ina case in which a large amount of

sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized dowloads are occurring. The @nalyst also discovers a couple of WAP are using the same SSID, but they have non-siandard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?
(A). Evil twin
(B). Jamming
(C). DNS poisoning
(D). Bluesnarfing
(E). DDoS
Answer: A

NO.669 A company's security team received notice of a critical vulnerability affecting a high-profile device within the web infrastructure. The vendor patch was just made available online but has not yet been regression tested in development environments. In the interim, firewall rules were implemented to reduce the access to the interface affected by the vulnerability. Which of the following controls does this scenario describe?
(A). Deterrent
(B). Compensating
(C). Detective
(D). Preventive
Answer: B

NO.670 A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?
(A). Deploy an MDM solution.
(B). Implement managed FDE.
(C). Replace all hard drives with SEDs.
(D). Install DLP agents on each laptop.
Answer: B

NO.671 A security analyst is reviewing web-application logs and finds the following log:

```
https://www.comptia.org/contact-us/%3Ffile%3D..%2F..%2F..%2Fetc%2Fpasswd
```

Which of the following attacks is being observed?
(A). Directory traversal
(B). XSS
(C). CSRF
(D). On-path attack
Answer: A

NO.672 Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

(A). An RTO report
(B). Arisk register
(C). A business impact analysis
(D). An asset value register
Answer: B
E: A disaster recovery plan

NO.673 Adynamic application vulnerability scan identified that code injection could be performed using a web form. Which of the following will be the BEST remediation to prevent this vulnerability?
(A). Implement input validations.
(B). Deploy MFA.
(C). Utilize a WAF.
(D). Configure HIPS.
Answer: B

C

NO.674 An administrator needs to protect user passwords and has been advised to hash the passwords. Which of the following BEST describes what the administrator is being advised to do?
(A). Perform a mathematical operation on the passwords that will convert them into umgue stnngs
(B). Add extra data to the passwords so their length is increased, making them harder to brute force
(C). Store all passwords in the system in a rainbow table that has a centralized location
(D). Enforce the use of one-time passwords that are changed for every login session.
Answer: D

A

NO.675 A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time In the event of a failure, which being maindful of the limited available storage space?
(A). Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
(B). Implement different backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
(C). Implement nightly full backups every Sunday at 8:00 p.m
(D). Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00
Answer: B

D

NO.676 An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:
* Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
* Internal users in question were changing their passwords frequently during that time period.
* A jump box that several domain administrator users use to connect to remote devices was recently compromised.
* The authentication method used in the environment is NTLM.
Which of the following types of attacks is MOST likely being used to gain unauthorized access?
(A). Pass-the-hash
(B). Brute-force
(C). Directory traversal
(D). Replay

Answer: A

NO.677 A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?
(A). IDS solution
(B). EDR solution
(C). HIPS software solution
(D). Network DLP solution
Answer: D

NO.678 Ahelp desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?
(A). Check the metadata in the email header of the received path in reverse order to follaw the email's path.
(B). Hover the mouse over the CIO's email address to verify the email address.
(C). Look at the metadata in the email header and verify the "From." line matches the CIO's email address.
(D). Forward the email to the CIO and ask if the CIO sent the email requesting the documents.
Answer: B
A

NO.679 Which of the following is a known security nsk associated with data archives that contain financial information?
(A). Data can become a liability if archived longer than required by regulatory guidance
(B). Data must be archived off-site to avoid breaches and meet business requirements
(C). Companies are prohibited from providing archived data to e-discovery requests
(D). Unencrypted archives should be preserved as long as possible and encrypted
Answer: A

NO.680 An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following should the organization consider before implementation? (Select TWO).
(A). The back-end directory source
(B). The identity federation protocol
(C). The hashing method
(D). The encryption method
(E). The registration authority
(F). The certificate authority
Answer: C,F
BD

NO.681 A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?
(A). Rainbow table attack
(B). Password spraying
(C). Logic bomb

(D). Malware bot

Answer: B

Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

NO.682 Which of the following techniques eliminates the use of rainbow tables for password cracking?

(A). Hashing

(B). Tokenization

(C). Asymmetric encryption

(D). Salting

Answer: D

Rainbow table attacks can easily be prevented by using salt techniques, which is a random data that is passed into the hash function along with the plain text.

NO.683 A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

(A). Log enrichment

(B). Log aggregation

(C). Log parser

(D). Log collector

Answer: D

NO.684 When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

(A). Acceptance

(B). Mitigation

(C). Avoidance

(D). Transference

Answer: D

Risk Transference refers to the shifting of the burden of loss for a risk to another party through legislation, contract, insurance or other means. https://www.bcmpedia.org/wiki/Risk_Transference

NO.685 An n that has a large number of mobile devices is explonng enhanced secunty controls to manage unauthonzed access if a device is lost or stolen. Specifically, mobile devices are mor than dmi (4 8km) from the busding, the management team would like to have the secunty team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

(A). Geofencing

(B). Lockout

(C). Near-field communication

(D). GPS tagging

Answer: A

NO.686 A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?
(A). Change the default settings on the PC.
(B). Define the PC firewall rules to limit access.
(C). Encrypt the disk on the storage device.
(D). Plug the storage device in to the UPS
Answer: B C

NO.687 A company is auditing the manner in which its European customers' personal information is handled Which of the following should the company consult?
(A). GDPR
(B). ISO
(C). NIST
(D). PCI DSS
Answer: A

NO.688 A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement Which of the following tools if available on the server, will provide the MOST useful information for the next assessment step?
(A). Autopsy
(B). Cuckoo
(C). Memdump
(D). Nmap
Answer: D
Nmap is basically mapping a network. The purpose of lateral pivoting is to gain a new perspective, or new information that will allow you to either privilege escalate, or to achieve the goal of the attack. If the compromised server the pen tester is exploiting has nmap enabled, the pen tester will be able to get an in-depth inside view of the internal network structure.

NO.689 An attacked is attempting to exploit users by creating a fake website with the URL www.validwebsite.com.
The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?
(A). Information elicitation
(B). Type squatting
(C). Impersonation
(D). Watering-hole attack
Answer: D B

NO.690 An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

(A). Require a complex, eight-character password that is updated every 90 days.
(B). Perform only non-intrusive scans of workstations.
(C). Use non-credentialed scans against high-risk servers.
(D). Log and alert on unusual scanner account logon times.
Answer: D

NO.691 After a recent security incident, a security analyst discovered that unnecessary ports were open on a firewall policy for a web server. Which of the following firewall policies would be MOST secure for a web server?
A)

[Source	Destination	Port	Action]
Any	Any	TCP 53	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

B)

[Source	Destination	Port	Action]
Any	Any	TCP 53	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

C)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Deny
Any	Any	TCP 443	Allow
Any	Any	Any	Allow

D)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Deny

(A). Option A
(B). Option B
(C). Option C
(D). Option D
Answer: D

NO.692 A startup company is using multiple SaaS and IaaS platform to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?
(A). SIEM
(B). DLP

(C). CASB
(D). SWG
Answer: C
A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies A CASB has a separate, and more distinctive role. Differing from the use case for SWG, which focuses on the broader filtering and protection against inbound threats and filtering illegitimate web traffic, a CASB is more deeply integrated and has control over your cloud application usage. It can be tied into an applications API to scan data at rest or can be used with a proxy based deployment to enforce inline policies for more real time protection.

NO.693 An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?
(A). SIEM
(B). SOAR
(C). EDR
(D). CASB
Answer: B

NO.694 An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?
(A). Date of birth
(B). Fingerprints
(C). PIN
(D). TPM
Answer: B

NO.695 Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?
(A). Least privilege
(B). Awareness training
(C). Separation of duties
(D). Mandatory vacation
Answer: C

NO.696 Which of the following BEST explains the difference between a data owner and a data custodian?
(A). The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
(B). The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
(C). The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
(D). The data owner grants the technical permissions for data access, while the data custodian

maintains the database access controls to the data
Answer: B

NO.697 Which of the following would cause a Chief information Security Officer the MOST concer regarding newly installed Internet-accessible 4K surveillance cameras?
(A). An inability to monitor 100% of every facility could expose the company to unnecessary risk.
(B). The cameras could be compromised if not patched in a timely manner.
(C). Physical security at the facility may not protect the cameras from theft.
(D). Exported videos may take up excessive space on the file servers.
Answer: C B

NO.698 A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?
(A). Asymmetric
(B). Symmetric
(C). Homomorphic
(D). Ephemeral
Answer: B C

NO.699 A SOC is currently being outsourced. Which of the following is being used?
(A). Microservice
(B). SaaS
(C). MSSP
(D). PaaS
Answer: C

NO.700 Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?
(A). Vulnerabilities with a CVSS score greater than 6.9.
(B). Critical infrastructure vulnerabilities on non-IP protocols.
(C). CVEs related to non-Microsoft systems such as printers and switches.
(D). Missing patches for third-party software on Windows workstations and servers.
Answer: B D

NO.701 Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?
(A). Intellectual property theft
(B). Elevated privileges
(C). Unknown backdoor
(D). Quality assurance
Answer: C

NO.702 A security analyst has been asked to investigate a situation after the SOC started to receive

alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

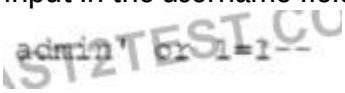
name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?
(A). Credential harvesting
(B). Keylogger
(C). Brute-force
(D). Spraying
Answer: D
Brute forcing focuses intensively on one account with every computable password attempt, whereas spraying simply attempts a few or several passwords on an account before moving on.

NO.703 Whichppf the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?
(A). Stored procedures
(B). Buffer overflows
(C). Data bias
(D). Code reuse
Answer: A
C

NO.704 A social media company based in North Amenca is looking to expand into new global markets and needs to maintain compliance with international standards With which of the following is the company's data protection officer MOST likely concerned''
(A). NIST Framework
(B). ISO 27001
(C). GDPR
(D). PCI-DSS
Answer: B
C

NO.705 A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:



Which of the following BEST explains this type of attack?
(A). DLL injection to hijack administrator services
(B). SQLi on the field to bypass authentication
(C). Execution of a stored XSS on the website
(D). Code to execute a race condition on the server
Answer: C D

NO.706 Which of the following would BEST provide detective and corrective controls for thermal regulation?
(A). A smoke detector
(B). A fire alarm
(C). An HVAC system
(D). A fire suppression system
(E). Guards
Answer: C
What are the functions of an HVAC system?
An HVAC system is designed to control the environment in which it works. It achieves this by controlling the temperature (THERMAL) of a room through heating and cooling. It also controls the humidity level in that environment by controlling the movement and distribution of air inside the room. So it provides detective and corrective controls for THERMAL regulation.

NO.707 A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:
* The devices will be used internationally by staff who travel extensively.
* Occasional personal use is acceptable due to the travel requirements.
* Users must be able to install and configure sanctioned programs and productivity suites.
* The devices must be encrypted
* The devices must be capable of operating in low-bandwidth environments.
Which of the following would provide the GREATEST benefit to the security posture of the devices?
(A). Configuring an always-on VPN
(B). Implementing application whitelisting
(C). Requiring web traffic to pass through the on-premises content filter
(D). Setting the antivirus DAT update schedule to weekly
Answer: A

NO.708 A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?
(A). Reverse proxy
(B). NIC teaming

(C). Load balancer
(D). Forward proxy
Answer: B C

NO.709 A Chief Information Security Officer (CISO) is evaluating (he dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system, selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system Which of the following is the CISO using to evaluate Hie environment for this new ERP system?
(A). The Diamond Model of Intrusion Analysis
(B). CIS Critical Security Controls
(C). NIST Risk Management Framevtoik
(D). ISO 27002
Answer: D

NO.710 An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?
(A). Web log files
(B). Browser cache
(C). DNS query logs
(D). Antivirus
Answer: C

NO.711 A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?
(A). DLP
(B). CASB
(C). HIDS
(D). EDR
(E). UEFI
Answer: A

NO.712 The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?
(A). Updating the playbooks with better decision points
(B). Dividing the network into trusted and untrusted zones
(C). Providing additional end-user training on acceptable use
(D). Implementing manual quarantining of infected hosts
Answer: A

NO.713 Data exftitration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have

determined that the system configuration notes were stored in the database administrator's folder on the web server Which of the following attacks explains what occurred? (Select TWO)
(A). Pass-the- hash
(B). Directory traversal
(C). SQL injection
(D). Privilege escalation
(E). Cross-site scnpting
(F). Request forgery
Answer: A,D BF

NO.714 Which of the following explains why RTO is included in a BIA?
(A). It identifies the amount of allowable downtime for an application or system,
(B). It prioritizes risks so the organization can allocate resources appropriately,
(C). It monetizes the loss of an asset and determines a break-even point for risk mitigation.
(D). It informs the backup approach so that the organization can recover data to a known time.
Answer: A

NO.715 Which of the following would an organizaton use to assign a value to risks based on probability of occurrence and impact?
(A). Risk matrix
(B). Risk register
(C). Risk appetite
(D). Risk mitgation plan
Answer: B

NO.716 A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site Upon investigation, a security analyst the identifies the following:
* The legitimate websites IP address is 10.1.1.20 and eRecruit local resolves to the IP
* The forged website's IP address appears to be 10.2.12.99. based on NetFtow records
* AH three at the organization's DNS servers show the website correctly resolves to the legitimate IP
* DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.
Which of the following MOST likely occurred?
(A). A reverse proxy was used to redirect network traffic
(B). An SSL strip MITM attack was performed
(C). An attacker temporarily pawned a name server
(D). An ARP poisoning attack was successfully executed
Answer: B

NO.717 An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?
(A). Antivirus
(B). IPS.
(C). FTP
(D). FIM

Answer: D

NO.718 A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?
(A). A bot
(B). A fileless virus
(C). A logic bomb
(D). A RAT
Answer: D
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.

NO.719 An enterprise to keep cryptpgraphic keys in a sade manner.Whihc of the fikkowug network appliances can achieve this goals?
(A). HSM
(B). CASB
(C). TPM
(D). DLP
Answer: A

NO.720 he SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?
(A). The NOC team
(B). The vulnerability management team
(C). The CIRT

Answer: C
D, The red team

NO.721 A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department Which of the following account types Is MOST appropriate for this purpose?
(A). Service
(B). Shared
(C). eneric
(D). Admin
Answer: A

NO.722 A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?
(A). A IaaS
(B). PaaS
(C). XaaS
(D). SaaS
Answer: B

A

NO.723 Which of the following control sets should a well-written BCP include? (Select THREE)
(A). Preventive
(B). Detective
(C). Deterrent
(D). Corrective
(E). Compensating
(F). Physical
(G). Recovery
Answer: A,D,G

NO.724 Whictpof the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?
(A). Stored procedures
(B). Buffer overflows
(C). Data bias
(D). Code reuse
Answer: A

C

NO.725 A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website The malicious actor posted an entry in an attempt to trick users into cltckmg the following:

https://www.c0mptla.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E

Which of the following was MOST likely observed?
(A). DLL injection
(B). Session replay
(C). SOLI
(D). XSS
Answer: B

D

NO.726 A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:
(A). whaling.
(B). smishing.
(C). spear phishing
(D). vishing
Answer: C

NO.727 A secunity engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks. Which of the following should the engineer implement?
(A). An air gap
(B). A hot site
(C). A VUAN
(D). A screened subnet
Answer: D

NO.728 An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps Which of the following control types has the organization implemented?
(A). Compensating
(B). Corrective
(C). Preventive
(D). Detective
Answer: C
D
the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. Compensating means to substitute one control with another (not happened here), Corrective means the attack has already happened (no mentioning), and detective is incorrect because the detective control detects ATTACKS, not vulnerabilities.

NO.729 A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST descnbes this technique?
(A). Vishing
(B). Whaling
(C). Phishing
(D). Smishing
Answer: D

*NO.730 A company acquired several other small companies The company thai acquired the others is transitioning network services to the cloud The company wants to make sure that performance and security remain intact Which of the following BEST meets both requirements?
(A). High availability
(B). Application security
(C). Segmentation
(D). Integration and auditing
Answer: A
High availability refers to the ability of a system or service to remain operational and available to users with minimal downtime. By ensuring high availability, the company can maintain good performance and ensure that users have access to the network services they need. High availability can also improve security, as it helps to prevent disruptions that could potentially be caused by security incidents or other issues.

NO.731 An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?
(A). DNS cache poisoning
(B). Domain hijacking
(C). Distributed denial-of-service
(D). DNS tunneling
Answer: D

A

NO.732 Which of the following should a data owner require all personnel to sign to legally protect intellectual property?
(A). An AUP
(B). An MOU
(C). An ISA
(D). An NDA
Answer: B

D

NO.733 Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?
(A). Test
(B). Staging
(C). Development
(D). Production
Answer: A

NO.734 A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?
(A). Reverse proxy
(B). Automated patch management
(C). Snapshots
(D). NIC teaming
Answer: A
A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

NO.735 Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?
(A). Something you exhibit
(B). Something you can do

(C). Someone you know
(D). Somewhere you are
Answer: D

NO.736 Which of the following is the purpose of a risk register?
(A). To define the level or risk using probability and likelihood
(B). To register the risk with the required regulatory agencies
(C). To identify the risk, the risk owner, and the risk measures
(D). To formally log the type of risk mitigation strategy the organization is using
Answer: C

NO.737 An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?
(A). TLS
(B). PFS
(C). ESP
(D). AH
Answer: A

NO.738 A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).
(A). head
(B). Tcpdump
(C). grep
(D). rail
(E). curl
(F). openssi
(G). dd
Answer: A,C
A - "analyst needs to review the first transactions quickly"
C - "search the entire series of requests for a particular string"

NO.739 A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:
(A). Dictionary
(B). Credential-stuffing
(C). Password-spraying
(D). Brute-forcea
Answer: D

NO.740 Some laptops recently went missing from a locked storage area that is protected by keyless

RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?
(A). The employee's physical access card was cloned.
(B). The employee is colluding with human resources
(C). The employee's biometrics were harvested
(D). A criminal used lock picking tools to open the door.
Answer: A

NO.741 Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media restriction policy?
(A). Putting security/antitamper tape over USB ports logging the port numbers and regularly inspecting the ports
(B). Implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced
(C). Placing systems into locked key-controlled containers with no access to the USB ports
(D). Installing an endpoint agent to detect connectivity of USB and removable media
Answer: B C

NO.742 A bank detects fraudulent activity on user's account. The user confirms transactions completed yesterday on the bank's website at https:/Awww.company.com. A security analyst then examines the user's Internet usage logs and observes the following output:

```
date;username;url;destinationport;responsecode
2020-03-01;userann;http://www.company.org/;80;302
2020-03-01;userann;http://www.company.org/secure_login/;80;200
2020-03-01;userann;http://www.company.org/dashboard/;80;200
```


Which of the following has MOST likely occurred?
(A). Replay attack
(B). SQL injection
(C). SSL stripping
(D). Race conditions
Answer: A

NO.743 A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following solutions BEST fits this use case?
(A). EDR
(B). DLP
(C). NGFW
(D). HIPS
Answer: A
The acronym EDR stands for Endpoint Detection and Response and is also known as EDTR. It is an endpoint security solution that is responsible for continuous monitoring of endpoints. This permanent monitoring enables the technology to detect and respond to cyber threats such as malware or ransomware at an early stage. The basis for this is always the analysis of context-related

information, which can be used to make corrective proposals for recovery.

NO.744 he Chief Information Secunty Officer came across a news arbcle outining a mechan'sm thal allows certan OS passwords to be bypassed The security team was then tasked with determining which method could be used to prevent data loss in the corporate environment in case an attacker bypasses authentication Which of the following will accomplish this objective?
(A). FDE
(B). Proper patch management protocols
(C). TPM
(D). Input validations
Answer: A

NO.745 Digital signatures use asymmetric encryption. This means the message is encrypted with:
(A). the sender's private key and decrypted with the sender's public key
(B). the sender's public key and decrypted with the sender's private key
(C). the sender's private key and decrypted with the recipient's public key.
(D). the sender's public key and decrypted with the recipient's private key
Answer: C
A

NO.746 A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?
(A). Security information and event management
(B). A web application firewall
(C). A vulnerability scanner
(D). A next-generation firewall
Answer: A

NO.747 A secunty engineer needs to build @ solution to satisty regulatory requirements that stale certain critcal servers must be accessed using MFA However, the critical servers are older and are unable to support the addition of MFA, Which of te following will the engineer MOST likely use to achieve this objective?
(A). A forward proxy
(B). A statetul frewail
(C). A jump server
(D). A port tap
Answer: C
B

NO.748 A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?
(A). Hacktivists
(B). White-hat hackers
(C). Script kiddies
(D). Insider threats
Answer: A

NO.749 An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?
(A). Antivirus
(B). IPS.
(C). FTP
(D). FIM
Answer: D

NO.750 A company i working on mobile device security afer a report revealed that users granted non-verified sofware access to corporate dat a. Which of the folowing ts the MOST effective security control to mitigate this risk?
(A). Block access to application stores.
(B). Implement OTA updates
(C). Update the BYOD pot
(D). Deploy a urttoem firmware
Answer: A

NO.751 A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?
(A). Segmentation
(B). Firewall whitelisting
(C). Containment
(D). isolation
Answer: A

NO.752 A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?
(A). MTBF
(B). RPO
(C). RTO
(D). MTTR
Answer: C D

NO.753 A company recently experienced an attack in which a malicious actor was able to exfiltrate data by cracking stolen passwords, using a rainbow table the sensitive dat a. Which of the following should a security engineer do to prevent such an attack in the future?
(A). Use password hashing.
(B). Enforce password complexity.
(C). Implement password salting.
(D). Disable password reuse.
Answer: B D

NO.754 A major palitical party experienced a server breach. The hacker then publicly posted stolen intemal cammunications compeming campaign strategies to give the oppasitian party an advantage. Which of the following BEST describes these threat actors?
(A). Semi-aulhorized hackers
(B). State actors
(C). Script kiddies
(D). Advanced persistent threats
Answer: B

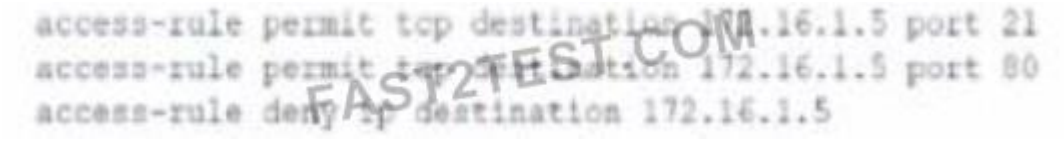
NO.755 A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?
(A). Private cloud
(B). Hybrid environment
(C). Managed security service provider
(D). Hot backup site
Answer: B

NO.756 A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?
(A). Autopsy
(B). Memdump
(C). FTK imager
(D). Wireshark
Answer: D
Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

NO.757 A recent security audit reveaied that @ popular website with IP address 172.16 1 also has an FTP service thal employees were using to store sensitive corporate dat a. The organization's outbound firewall processes rules top-down. Which of the following would permit HTTP and HTTPS, while denying all other services for this host?
(A).

(B).

(C).



(D).

Answer: A

D

NO.758 A user enters a password to log in to a workstation and is then prompted to enter an authentication code.
Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).
(A). Something you know
(B). Something you have
(C). Somewhere you are
(D). Someone you are
(E). Something you are
(F). Something you can do
Answer: B,E

AB

NO.759 A tax organization is working on a solution to validate the online submission of documents The solution should be earned on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?
(A). User certificate
(B). Self-signed certificate
(C). Computer certificate
(D). Root certificate
Answer: D

A

NO.760 A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?
(A). Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
(B). Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
(C). Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
(D). Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.
Answer: B

D

NO.761 A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security

analyst to gather information and confirm it is a malicious document without executing any code it may contain?
(A). Open the document on an air-gapped network
(B). View the document's metadata for origin clues
(C). Search for matching file hashes on malware websites
(D). Detonate the document in an analysis sandbox
Answer: D

C

NO.762 After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?
(A). The unexpected traffic correlated against multiple rules, generating multiple alerts.
(B). Multiple alerts were generated due to an attack occurring at the same time.
(C). An error in the correlation rules triggered multiple alerts.
(D). The SIEM was unable to correlate the rules, triggering the alerts.
Answer: A

NO.763 Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?
(A). Pulverizing
(B). Shredding
(C). Incinerating
(D). Degaussing
Answer: D

B

NO.764 A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?
(A). SPIM
(B). Vishing
(C). Spear phishing
(D). Smishing
Answer: D

NO.765 A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works BEST until a proper fix is released?
(A). Detective
(B). Compensating
(C). Deterrent
(D). Corrective
Answer: A

B

NO.766 A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadat a. Which of the following would be part of the images if all the metadata is still intact?
(A). The GPS location
(B). When the file was deleted

(C). The total number of print jobs
(D). The number of copies made
Answer: A

NO.767 An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has sont insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE).
(A). SFTP, FTPS
(B). SNMPv2, SNMPv3
(C). HTTP, HTTPS
(D). TEIP, FIP
(E). SNMPv1, SNMPv2
(F). Telnet, SSH
(G). TLS, SSL
(H). POP, IMAP
(I). Login, rlogin
Answer: A,E,G BCF

NO.768 A developer is concerned about people downloading fake malware-infected replicas of a popular game. Which of the following should the developer do to help verify legitimate versions of the game for users?
(A). Digitally sign the relevant game files.
(B). Embed a watermark using steganography.
(C). Implement TLS on the license activation server.
(D). Fuzz the application for unknown vulnerabilities.
Answer: A

NO.769 Which of the following prevents an employee from seeing a colleague who is visting an inappropriate website?
(A). Job roration policy
(B). NDA
(C). AUP
(D). Separation of duties policy
Answer: C

NO.770 After entering a username and password, and administrator must draw a gesture on a touch screen. Which of the following demonstrates what the administrator is providing?
(A). Multifactor authentication
(B). Something you can do
(C). Biometric
(D). Two-factor authentication

Answer: D

NO.771 A security analyst Is hardening a Linux workstation and must ensure It has public keys forwarded to remote systems for secure login Which of the following steps should the analyst

perform to meet these requirements?
(Select TWO).
(A). Forward the keys using ssh-copy-id.
(B). Forward the keys using scp.
(C). Forward the keys using ash -i.
(D). Forward the keys using openssl -s.
(E). Forward the keys using ssh-keyger.
Answer: A,D

NO.772 Which of the following is a benefit of including a risk management framework into an organization's security approach?
(A). It defines expected service levels from participating supply chain partners to ensure system outages are remediated in a timely manner
(B). It identifies specific vendor products that have been tested and approved for use in a secure environment.
(C). It provides legal assurances and remedies in the event a data breach occurs
(D). It incorporates control, development, policy, and management activities into IT operations.
Answer: D

NO.773 Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?
(A). Watering-hole attack
(B). Credential harvesting
(C). Hybrid warfare
(D). Pharming
Answer: A

NO.774 A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?
(A). The examiner does not have administrative privileges to the system
(B). The system must be taken offline before a snapshot can be created
(C). Checksum mismatches are invalidating the disk image
(D). The swap file needs to be unlocked before it can be accessed
Answer: A

NO.775 A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)
(A). An air gap
(B). A cold aisle
(C). Removable doors
(D). A hot aisle
(E). An IoT thermostat
(F). A humidity monitor
Answer: E,F BD

NO.776 A securtly analyst wants to reference a standard to develop a risk management program. Which af the following ts the BEST source for the analyst to use?
(A). SSAE SOC 2
(B). SO 31000
(C). NIST CSF
(D). GDPR
Answer: B

NO.777 The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?
(A). SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
(B). SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
(C). SSO would reduce the password complexity for frontline staff.
(D). SSO would reduce the resilience and availability of system if the provider goes offline.
Answer: D

NO.778 A compart jut heplmanieg 6 new tlewor ploy thet owe eriptoyens f wee personel doce or ocala and fe aherag wo wong tow howe. Some of ie
* Employees must provide an alternate work location (i.e., a home address)
* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.
Which of the following BEST describes the MDM options the company is using?
(A). Geofencing, content management, remote wipe, containerization, and storage segmentation
(B). Content management, remote wipe, geolocation, context-aware authentication, and containerization
(C). Application management, remote wipe, geofencing, context-aware authentication, and containerization
(D). Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption
Answer: D B

NO.779 Two hospitals merged into a single organization. The privacy officer requested a review of ait records to ensure encryption was used Guring record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?
(A). Personal heath information
(B). Personally Kentifiable information
(C). Tokenized data
(D). Proprietary data
Answer: B A

NO.780 A security engineer needs to select a primary authentication source for use with a client

application. The application requires the user to log in with a username, password, and, when needed, a challenge response. Which of the follwing solutions BEST meets this requirement?
(A). PSK
(B). LDAP
(C). RADIUS
(D). PAP
Answer: B

NO.781 An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?
(A). Social media
(B). Cloud
(C). Supply chain
(D). Social engineering
Answer: D

C

NO.782 A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```


Which of the following attacks was successfully implemented based on the output?
(A). Memory leak
(B). Race conditions
(C). SQL injection
(D). Directory traversal
Answer: D

NO.783 A cloud service provider has created an environment where customers can connect existing local networks to the cloud for additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?
(A). Public
(B). Community
(C). Hybrid
(D). Private
Answer: C
Hybrid cloud refers to a mixed computing, storage, and services environment made up of on-premises infrastructure, private cloud services, and a public cloud-such as Amazon Web Services (AWS) or Microsoft Azure-with orchestration among the various platforms

NO.784 Which of the following control types would be BEST to use to identify violations and incidents?
(A). Detective

(B). Compensating
(C). Deterrent
(D). Corrective
(E). Recovery
(F). Preventive
Answer: A

NO.785 Which of the following incident response steps occurs before containment?
(A). Eradication
(B). Recovery
(C). Lessons learned
(D). Identification
Answer: D

NO.786 An organization has activated an incident response plan due to a malware outbreak on its network The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code Which of the following actions would be BEST to prevent reinfection from the initial infection vector?
(A). Prevent connections over TFTP from the internal network
(B). Create a firewall rule that blocks port 22 from the internet to the server
(C). Disable file shanng over port 445 to the server
(D). Block port 3389 inbound from untrusted networks
Answer: A

D

NO.787 An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?
(A). MDM
(B). MAM
(C). VDI
(D). DLP
Answer: A

NO.788 wo organizations are discussing a possible merger, Both organizations' Chief Financial Officers would like to safely share payroll data with each other to determine if the pay scales for different roles are similar at both organizations. Which of the following techniques would be BEST to protect employee data while allowing the companies to successfully share this information?
(A). Pseudo-anonymization
(B). Tokenization
(C). Data masking
(D). Encryption
Answer: C

D

NO.789 A multinational organization that offers web-based services has datacenters that are located

only in the United States; however, a large number of its customers are in Australia, Europe, and Chin a. Payments for services are managed bya third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?
(A). Payment Card Industry Data Security Standard
(B). Cloud Security Alliance Best Practices
(C). ISO/IEC 27032 Cybersecurity Guidelines
(D). General Data Protection Regulation
Answer: A

D

NO.790 A security monitoring company offers a service that alerts its customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?
(A). STIX
(B). The dark web
(C). TAXI
(D). Social media
(E). PCI
Answer: B

NO.791 A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?
(A). Randomize the shared credentials
(B). Use only guest accounts to connect.
(C). Use SSH keys and remove generic passwords
(D). Remove all user accounts.
Answer: C

NO.792 Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers?
accounts. Which of the following should be implemented to prevent similar situations in the future?
(A). Ensure input validation is in place to prevent the use of invalid characters and values.
(B). Calculate all possible values to be added together and ensure the use of the proper integer in the code.
(C). Configure the web application firewall to look for and block session replay attacks.
(D). Make sure transactions that are submitted within very short time periods are prevented from being processed.
Answer: A

NO.793 A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

(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
Answer: C

NO.794 To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?
(A). Install a hypervisor firewall to filter east-west traffic.
(B). Add more VLANs to the hypervisor network switches.
(C). Move exposed or vulnerable VMs to the DMZ.
(D). Implement a zero-trust policy and physically segregate the hypervisor servers.
Answer: B

NO.795 An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?
(A). It allows for the sharing of digital forensics data across organizations
(B). It provides insurance in case of a data breach
(C). It provides complimentary training and certification resources to IT security staff.
(D). It certifies the organization can work with foreign entities that require a security clearance
(E). It assures customers that the organization meets security standards
Answer: E

NO.796 A RAT that was used to compromise an organization's banking credentials was found on a user's computer.
The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?
(A). Create a new acceptable use policy.
(B). Segment the network into trusted and untrusted zones.
(C). Enforce application whitelisting.
(D). Implement DLP at the network boundary
Answer: C

NO.797 Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area?
(Select TWO).
(A). Barricades
(B). Thermal sensors
(C). Drones
(D). Signage
(E). Motion sensors
(F). Guards
(G). Bollards
Answer: A,E

NO.798 Which of the following processes will eliminate data using a method that will allow the storage device to be reused after the process is complete?
(A). Pulverizing
(B). Overwriting
(C). Shredding
(D). Degaussing
Answer: D
B
https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/

NO.799 An organization is tuning SIEM rules based off of threat intelligence reports. Which of the following phases of the incident response process does this scenario represent?
(A). Lessons learned
(B). Eradication
(C). Recovery
(D). Preparation
Answer: A

NO.800 Which of the following is the MOST effective way to detect security flaws present on third-party libraries embedded on software before it is released into production?
(A). Employ different techniques for server- and client-side validations.
(B). Use a different version control system for third-party libraries.
(C). Implement a vulnerability scan to assess dependencies earlier on SDLC.
(D). Increase the number of penetration tests before software release.
Answer: C

NO.801 A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?
(A). SINT
(B). SIEM
(C). CVSS
(D). CVE
Answer: D

NO.802 A network administrator al a large organization | reviewing methods lo improve the securty of the wired LAN, Any seourty improvement must be centrally managed and alow corporate-owned devices lo have access to the intranet bul limit others to Internet access only. Which of the following should the adeninistrator recommend?
(A). 802.1X ullizing the current PKI ifrastructure
(B). $50 to authenticate comorate users
(C). MAC address filtering with ACLs on the router
(D). PAM for user account management
Answer: A

NO.803 Aconbgany uses a drone for precise perimeter and boundary monitoring. Which of the

following should be MOST conceming to the company?
(A). Privacy
(B). Cloud storage of telemetry data
(C). GPS spoofing
(D). Weather events
Answer: C

NO.804 An organization just implemented a new security system. Local laws state that citizens must be notified prior to encountering the detection mechanism to deter malicious activities. Which of the following is being implemented?
(A). Proximity cards with guards
(B). Fence with electricity
(C). Drones with alarms
(D). Motion sensors with signage
Answer: D

NO.805 A forensics investigator is examining a number of unauthorized payments the 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:
<a href-"https://www.company.com/payto.do?routing=00001111&accc=22223334&amount-250">Click here to unsubscribe Which of the following will the forensics investigator MOST likely determine has occurred?
(A). SQL injection
(B). CSRF
(C). XSS
(D). XSRF
Answer: D

NO.806 A user forwarded a suspicious email to the security team, Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?
(A). Configure the web content filter for the web address.
(B). Report the website to threat intelligence partners
(C). Set me SIEM to alert for any activity to the web address.
(D). Send out a corporate communication to warn all users Of the malicious email.
Answer: A

NO.807 Which of the following corporate policies is used to help prevent employee fraud and to detect system log modifications or other malicious activity based on tenure?
(A). Background checks
(B). Mandatory vacation
(C). Social media analysis
(D). Separation of duties
Answer: B

NO.808 A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).
(A). The order of volatility
(B). A CRC32 checksum
(C). The provenance of the artifacts
(D). The vendor's name
(E). The date time
(F). A warning banner
Answer: A,E

NO.809 A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?
(A). SSO
(B). IDS
(C). MFA
(D). TPM
Answer: C

NO.810 A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN ?
(A). AH
(B). EDR
(C). ESP
(D). DNSSEC

Answer: C
https://www.hypr.com/encapsulating-security-payload-esp/
Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

NO.811 A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether odified in transit before installation on the user's computer. Which of the following can be used to safely assess the file?
(A). Check the hash of the installation file
(B). Match the file names
(C). Verify the URL download location
(D). Verify the code-signing certificate
Answer: A
The hardware manufacturer will post the hash of the file publicly, and anyone who receives a copy of that file will be able to run a checksum on the file themselves, and compare them to the official manufacturer-provided checksum. Hashing is almost always the correct answer in these type of questions. You'll see a lot of Github repositories using hashed checksums as well for verification, and I

recently just installed Java onto my new computer. Java provided me with a hashed checksum for the setup executable.

NO.812 A company Is concerned about ts securkty afler a red-tearn exercise. The report shows the team was able to reach the critical servers due to Ihe SMB being exposed fo the Internet and running NTLMV1, Which of the following BEST explains the findings?
(A). Default settings on the servers
(B). Unsecuted administrator accounts
(C). Open ports and services
(D). Weak Gata encryption
Answer: C

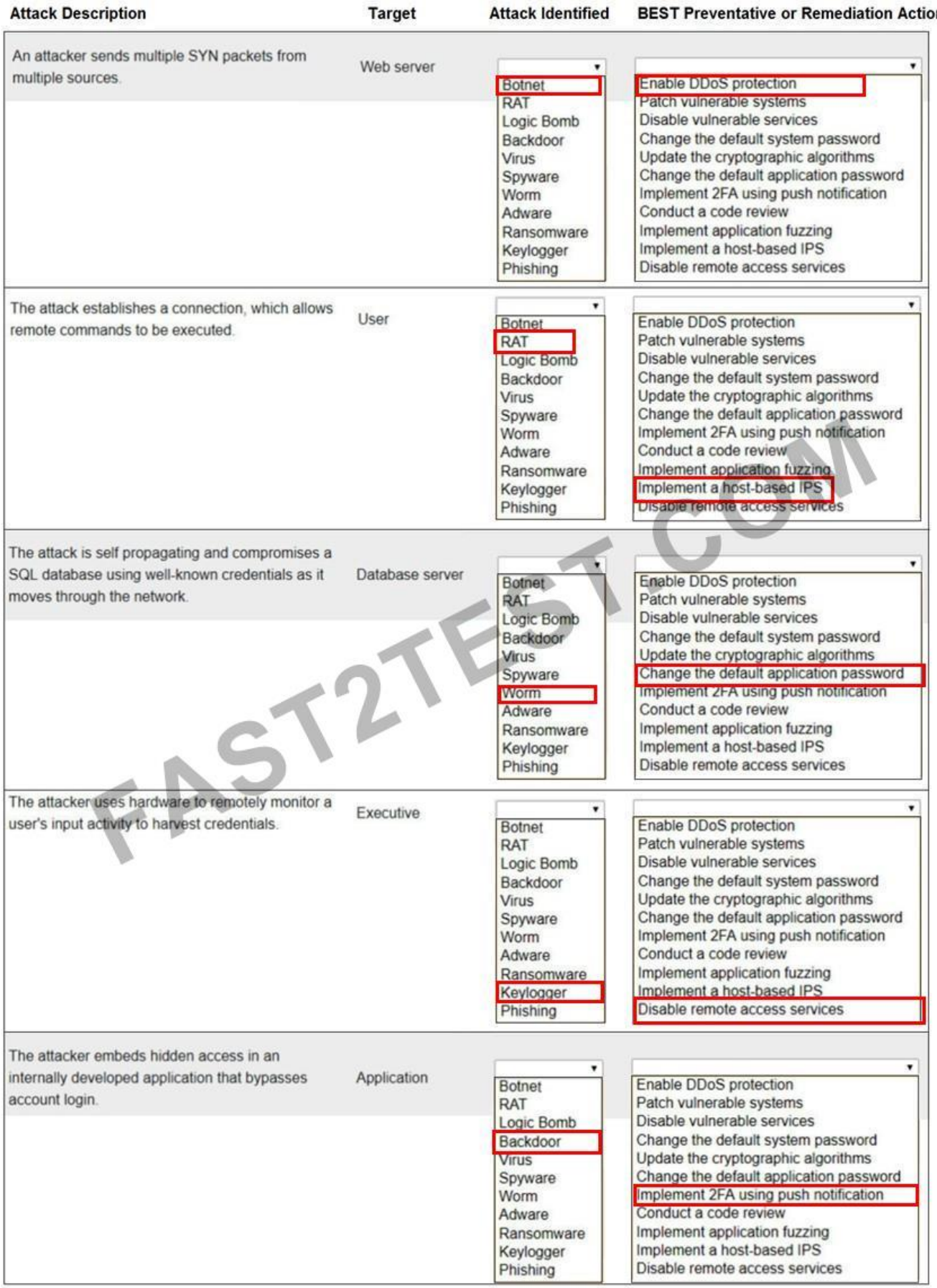
NO.813 To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials.
Which of the following will BEST ensure the site's users are not compromised after the reset?
(A). A password reuse policy
(B). Account lockout after three failed attempts
(C). Encrypted credentials in transit
(D). A geofencing policy based on login history
Answer: C

A

NO.814 Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

NO.815 A commercial cyber-threat intelligence organization observes IoCs across a variety of

unrelated customers.
Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:
(A). perform attribution to specific APTs and nation-state actors.
(B). anonymize any PII that is observed within the IoC data.
(C). add metadata to track the utilization of threat intelligence reports.
(D). assist companies with impact assessments based on the observed data
Answer: B

NO.816 A Chief Information Officer is concerned about employees using company-issued laptops lo steal data when accessing network shares. Which of the following should the company Implement?
(A). DLP
(B). CASB
(C). HIDS
(D). EDR
(E). UEFI
Answer: A
Chmod removes the setuido permission, that is, it removes the S bit. Setuido is the specific permission, but it is removed with Chmod. https://www.cbtnuggets.com/blog/technology/system-admin/linux-file-permissions-understanding-setuid-setgid-and-the-sticky-bit

NO.817 A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?
(A). Salting the magnetic strip information
(B). Encrypting the credit card information in transit.
(C). Hashing the credit card numbers upon entry.
(D). Tokenizing the credit cards in the database
Answer: C D

NO.818 A user's account is constantly being locked out. Upon further review, @ security analyst found the following in the SIEM:

Time	Log Message
9:00:00 AM	login: user password: aBG23TMV
9:00:01 AM	login: user password: aBG33TMV
9:00:02 AM	login: user password: aBG43TMV
9:00:03 AM	login: user password: aBG53TMV

Which of the following describes what is occurring?
(A). An attacker is utilizing a password-spraying attack against the account
(B). An attacker is utilizing a dictionary attack against the account
(C). An attacker is utilizing a brute-force attack against the account
(D). An attacker is utilizing a rainbow table attack against the account
Answer: B C

NO.819 A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?
(A). Race-condition
(B). Pass-the-hash
(C). Buffer overflow
(D). XSS
Answer: C

NO.820 A recent security breach exploited software vulnerabilities in the firewall and within the network management solution. Which of the following will MOST likely be used to identify when the breach occurred through each device?
(A). SIEM correlation dashboards
(B). Firewall syslog event logs
(C). Network management solution login audit logs
(D). Bandwidth monitors and interface sensors
Answer: A

NO.821 Which of the following organizations sets frameworks and controls for optimal security configuration on systems?
(A). ISO
(B). GDPR
(C). PCI DSS
(D). NIST
Answer: D

NO.822 During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of 12 months via the internet. The penetration tester stops the test to inform the client of the findings Which of the following should be the client's NEXT step to mitigate the issue''
(A). Conduct a full vulnerability scan to identify possible vulnerabilities
(B). Perform containment on the critical servers and resources
(C). Review the firewall and identify the source of the active connection
(D). Disconnect the entire infrastructure from the internet
Answer: D A

NO.823 A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?
(A). WAF
(B). CASB
(C). VPN
(D). TLS
Answer: B

NO.824 The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

(A). SSO
(B). MFA
(C). PKI
(D). OLP
Answer: A

NO.825 A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional dat a. Historically, this setup has worked without issue, but the researcher recently started getting the following message:
Which of the following network attacks is the researcher MOST likely experiencing?
(A). MAC cloning
(B). Evil twin
(C). Man-in-the-middle
(D). ARP poisoning
Answer: C

NO.826 During an incident response, a security analyst observes the following log entry on the web server.

```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experience?
(A). SQL injection
(B). Cross-site scripting
(C). Pass-the-hash
(D). Directory traversal
Answer: D

NO.827 The Chief information Securtty Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside cornpany. Additionally, the CISO would Ske this solution to provide the same protections even when a company laptop or mobile device ts away from # home office. Which of the following should the CISO choose?
(A). CASB
(B). Next-generation SWG
(C). NGFW
(D). Web-application firewall
Answer: A

B

NO.828 After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?
(A). IoT sensor
(B). Evil twin
(C). Rogue access point
(D). On-path attack

Answer: C

NO.829 A company is implementing a DLP solution on the file server. The file server has PII. financial information, and health information stored on it Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data Which of the following should the company do to help accomplish this goal?
(A). Classify the data
(B). Mask the data
(C). Assign an application owner
(D). Perform a risk analysis
Answer: A

NO.830 A systems administrator is looking for a solution that will help prevent OAuth applications from being leveraged by hackers to tick users into authonzing the use of their corporate credentials. Which of the following BEST describes this solution?
(A). CASB
(B). UEM
(C). WAF
(D). VPC
Answer: B C

NO.831 A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?
(A). It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
(B). It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
(C). It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
(D). It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach
Answer: A

NO.832 A network administrator has been asked to install an IDS to improve the security posture of an organization.
Which of the following control types is an IDS?
(A). Corrective
(B). Physical
(C). Detective
(D). Administrative
Answer: C

NO.833 A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate

this concern?
(A). Create consultant accounts for each region, each configured with push MFA notifications.
(B). Create one global administrator account and enforce Kerberos authentication
(C). Create different accounts for each region. limit their logon times, and alert on risky logins
(D). Create a guest account for each region. remember the last ten passwords, and block password reuse
Answer: C
https://www.crowdstrike.com/blog/service-accounts-performing-interactive-logins/

NO.834 As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?
(A). Creating a playbook within the SOAR
(B). Implementing rules in the NGFW
(C). Updating the DLP hash database
(D). Publishing a new CRL with revoked certificates
Answer: A

NO.835 An analyst receives multiple alerts for beaconing activity for a host on the network, After analyzing the activity, the analyst observes the following activity:
* A user enters comptia.org into a web browser.
* The website that appears is not the comptia.org site.
* The website is a malicious site from the attacker.
* Users in a different office are not having this issue.
Which of the following types of attacks was observed?
(A). On-path attack
(B). DNS poisoning
(C). Locator (URL) redirection
(D). Domain hijacking
Answer: C B

NO.836 A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?
(A). Role-based access control
(B). Discretionary access control
(C). Mandatory access control
(D). Attribute-based access control
Answer: B
Discretionary access control (DAC) is a model of access control based on access being determined "by the owner" of the resource in question. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have.

NO.837 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
Answer: A
Phishing
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20or%20fear%20in%20victims.

NO.838 The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:
* Users to choose a password unique to their last ten passwords
* Users to not log in from certain high-risk countries
Which of the following should the security team implement? (Select TWO).
(A). Password complexity
(B). Password history
(C). Geolocation
(D). Geofencing
(E). Geotagging
(F). Password reuse
Answer: A,B

BC

NO.839 A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation which improves conditions, but performance degrades again after a few days. The administrator runs an anarysis tool and sees the following output:

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```


The administrator terminates the timeAttend.exe observes system performance over the next few days, and notices that the system performance does not degrade Which of the following issues is MOST likely occurring?
(A). DLL injection
(B). API attack
(C). Buffer oveiflow
(D). Memory leak
Answer: C

D

NO.840 A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?
(A). The Diamond Mode! of Intrusion Analysis

(B). The Cyber Kill Chain e
(C). The MITRE CVE database
(D). The incident response process
Answer: C

A

NO.841 A security analyst sees the following log output while reviewing web logs:

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?
(A). Secure cookies
(B). Input validation
(C). Code signing
(D). Stored procedures
Answer: B

NO.842 Server administrators want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently across a number or virtual servers. They also need to avoid potential dental-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?
(A). Dynamic resource allocation
(B). High availably
(C). Segmentation
(D). Container security
Answer: A

NO.843 A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public are a. Which of the following would MOST likely have prevented this breach?
(A). A firewall
(B). A device pin
(C). A USB data blocker
(D). Biometrics
Answer: C
https://www.promorx.com/blogs/blog/how-does-a-usb-data-blocker-work Connecting via the data port of your mobile device, the Data Blockers creates a barrier between your mobile device and the charging station. Your phone will draw power as usual, allowing you to use it normally and charge it at the same time, but this clever piece of equipment will prevent any data exchange.
"Malicious USB charging cables and plugs are also a widespread problem. As with card skimming, a device may be placed over a public charging port at airports and other transit locations. A USB data blocker can provide mitigation against these juice- jacking attacks by preventing any sort of data transfer when the smartphone or laptop is connected to a charge point "

NO.844 Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

(A). MSSP
(B). Public cloud
(C). Hybrid cloud
(D). Fog computing
Answer: C

D

NO.845 A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?
(A). OAuth
(B). SSO
(C). SAML
(D). PAP
Answer: C

NO.846 n attack relies on an end user visiting a website the end user would typically visit; however, the site is compromised and uses vulnerabilities in the end user's browser to deploy malicious software. Which of the following types of attack does this describe?
(A). Smishing
(B). Whaling
(C). Watering hole
(D). Phishing
Answer: C

*
NO.847 Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?
(A). Penetration testing
(B). Code review
(C). Wardriving
(D). Bug bounty
Answer: A

NO.848 Which of the following describes the continuous delivery software development methodology?
(A). Waterfall
(B). Spiral
(C). V-shaped
(D). Agile
Answer: D

NO.849 An organization is building backup server rooms in geographically diverse locations The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room Which of the following should the systems engineer consider?
(A). Purchasing hardware from different vendors
(B). Migrating workloads to public cloud infrastructure
(C). Implementing a robust patch management solution

(D). Designing new detective security controls
Answer: A

NO.850 Which of the following can be used by a monitoring tool to compare values and detect password leaks without providing the actual credentials?
(A). Hashing
(B). Tokenization
(C). Masking
(D). Encryption
Answer: A
https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/

NO.851 A penetration tester gains access to a network by exploiting a vulnerability on a public-facing web server. Which of the following techniques will the tester most likely perform NEXT?
(A). Gather more Information about the target through passive reconnaissance.
(B). Establish rules of engagement before proceeding.
(C). Create a user account to maintain persistence.
(D). Move laterally throughout the network to search for sensitive information.
Answer: C

NO.852 Which of the following typically uses a combination of human and artificial intelligence to analyze event data and take action without intervention?
(A). TTP
(B). OSINT
(C). SOAR
(D). SIEM
Answer: C

NO.853 user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is fully patched. The user downloaded a driver package from the Internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is the MOST likely cause of the infection?
(A). The dnver had malware installed and was refactored upon download to avoid detection
(B). The user's computer had a rootkit installed that had avoided detection until the new dnver overwrote key files.
(C). The user's antivirus software definitions were out of date and were damaged by the installation of the driver.
(D). The user's computer had been infected with a logic bomb set to run when new dnver was installed.
Answer: A

B

NO.854 Which of the following is a targeted attack aimed at compromising users within a specific industry or group?
(A). Watering hole
(B). Typosquatting
(C). Hoax

(D). Impersonation

Answer: A

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses. Background Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. Targeted attacks differ from traditional online threats in many ways: * Targeted attacks are typically conducted as campaigns. APTs are often conducted in campaigns-a series of failed and successful attempts over time to get deeper and deeper into a target's network-and are thus not isolated incidents. * They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft. Attackers often customize, modify and improve their methods depending on the nature of their target sector and to circumvent any security measures implemented. Phases of a Targeted Attack * Intelligence gathering. Threat actors identify and gather publicly available information about their target to customize their attacks. This initial phase aims to gain strategic information not only on the intended target's IT environment but also on its organizational structure. The information gathered can range from the business applications and software an enterprise utilizes to the roles and relationships that exist within it. This phase also utilizes social engineering techniques that leverage recent events, work-related issues or concerns, and other areas of interest for the intended target. * Point of entry. Threat actors may use varied methods to infiltrate a target's infrastructure. Common methods include customized spearphishing email, zero-day or software exploits, and watering hole techniques. Attackers also utilize instant-messaging and social networking platforms to entice targets to click a link or download malware. Eventually, establishing a connection with the target is acquired. * Command-and-control (C&C) communication. After security has been breached, threat actors constantly communicate to the malware to either execute malicious routines or gather information within the company network. Threat actors use techniques to hide this communication and keep their movements under the radar. * Lateral movement. Once inside the network, threat actors move laterally throughout the network to seek key information or infect other valuable systems. * Asset/Data Discovery. Notable assets or data are determined and isolated for future data exfiltration. Threat actors have access to "territories" that contain valuable information and noteworthy assets. These data are then identified and transferred through tools like remote access Trojans (RATs) and customized and legitimate tools. A possible technique used in this stage may be sending back file lists in different directories so attackers can identify what are valuable. * Data Exfiltration. This is the main goal of targeted attacks. An attack's objective is to gather key information and transfer this to a location that the attackers control. Transferring such data can be conducted quickly or gradually. Targeted attacks strive to remain undetected in the network in order to gain access to the company's crown jewels or valuable data. These valuable data include intellectual property, trade secrets, and customer information. In addition, threat actors may also seek other sensitive data such as top-secret documents from government or military institutions. Once a targeted attack is successful and has reached as far as the data exfiltration stage, it is not difficult for attackers to draw out the data. Although targeted attacks are not known to specifically target consumers, their data are also at risk once target business sectors have been infiltrated. As a result, such attacks (if successful) may damage a company's reputation.
https://www.trendmicro.com/vinfo/us/security/definition/targeted-

attacks#:~:text=A%20targeted%20attack%20refers%20to,over%20a%20long%2Dterm%20period.

NO.855 Which of the following is a detective and deterrent control against physical intrusions?
(A). Alock
(B). An alarm
(C). A fence
(D). Asign
Answer: B

NO.856 A security analyst is tasked with classifying data to be stored on company servers. Which of the following should be classified as proprietary?
(A). Customers' dates of birth
(B). Customers' email addresses
(C). Marketing strategies
(D). Employee salaries
Answer: C

NO.857 A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an Iv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?
(A). Context-aware authentication
(B). Simultaneous authentication of equals
(C). Extensive authentication protocol
(D). Agentless network access control
Answer: A
An access control scheme that verifies an object's identity based on various environmental factors, like time, location, and behavior.

NO.858 A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?
(A). Recovery
(B). Identification
(C). Lessons learned
(D). Preparation
Answer: C

NO.859 A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls Which of the following should be implemented to BEST address the CSO's concerns? {Select TWO)
(A). AWAF
(B). ACASB
(C). An NG-SWG
(D). Segmentation
(E). Encryption

(F). Containerization

Answer: B,F

BC

NO.860 A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing Employees who travel need their accounts protected without the nsk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?

(A). Enforce MFA when an account request reaches a nsk threshold

(B). Implement geofencing to only allow access from headquarters

(C). Enforce time-based login requests that align with business hours

(D). Shift the access control scheme to a discretionary access control

Answer: B

A

NO.861 A scurity analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:

* Ensure mobile devices can be tracked and wiped.

* Confirm mobile devices are encrypted.

Which of the following should the analyst enable on all the devices to meet these requirements?

(A). A Geofencing

(B). Biometric authentication

(C). Geolocation

(D). Geotagging

Answer: A

D

NO.862 The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

(A). install a smart meter on the staff WiFi.

(B). Place the environmental systems in the same DHCP scope as the staff WiFi.

(C). Implement Zigbee on the staff WiFi access points.

(D). Segment the staff WiFi network from the environmental systems network.

Answer: B

D

NO.863 A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

(A). SDP

(B). AAA

(C). IaaS

(D). MSSP

(E). Microservices

Answer: D

https://www.techtarget.com/searchitchannel/definition/MSSP

NO.864 During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

(A). The forensic investigator forgot to run a checksum on the disk image after creation
(B). The chain of custody form did not note time zone offsets between transportation regions
(C). The computer was turned off. and a RAM image could not be taken at the same time
(D). The hard drive was not properly kept in an antistatic bag when rt was moved
Answer: A

NO.865 An organization is planning lo open other data centers to sustain operations in the event of a natural disaster. Which of the following considerations would BEST support the organization's resiliency?
(A). Geographic dispersal
(B). Generator power
(C). Fire suppression
(D). Facility automation
Answer: A

NO.866 Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?
(A). A worm that has propagated itself across the intranet, which was initiated by presentation media
(B). A fileless virus that is contained on a vCard that is attempting to execute an attack
(C). A Trojan that has passed through and executed malicious code on the hosts
(D). A USB flash drive that is trying to run malicious code but is being blocked by the host firewall
Answer: A

NO.867 Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only.
In order to proceed past that banner. users must click the OK button. Which of the following is this an example of?
(A). AUP
(B). NDA
(C). SLA
(D). MOU
Answer: A

NO.868 The Chief information Security Officer wants to prevent exfilitration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?
(A). DLP
(B). USB data blocker
(C). USB OTG
(D). Disabling USB ports
Answer: C

B

NO.869 A security analyst is receiving numerous alerts reporting that the response time of an

internet-facing application has been degraded However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?
(A). DNS poisoning
(B). MAC flooding
(C). DDoS attack
(D). ARP poisoning
Answer: C

NO.870 A global pandemic is forcing a private organization to close some business units and reduce staffing at others.
Which of the following would be BEST to help the organization's executives determine the next course of action?
(A). An incident response plan
(B). A communications plan
(C). A disaster recovery plan
(D). A business continuity plan

Answer: D