Correct Answer: A

QUESTION 420
A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

A. Content filter
B. SIEM
C. Firewall rules
D. DLP

Correct Answer: C

QUESTION 421
A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).

A. HIDS
B. NIPS
C. HSM
D. WAF
E. NAC
F. NIDS
G. Stateless firewall

Correct Answer: DG
Explanation:
https://www.netscout.com/what-is-ddos

QUESTION 422
A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

- www.companysite.com
- shop.companysite.com
- about-us.companysite.com
- contact-us.companysite.com
- secure-logon.companysite.com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

A. A self-signed certificate
B. A root certificate
C. A code-signing certificate
D. A wildcard certificate
E. An extended validation certificate

Correct Answer: A

QUESTION 423
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Correct Answer: D

QUESTION 424
To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

Correct Answer: D
QUESTION 425
A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services
B. SQLi on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server

Correct Answer: B

QUESTION 426
Which of the following must be in place before implementing a BCP?

A. SLA
B. AUP
C. NDA
D. BIA

Correct Answer: D
Explanation:
To create an effective business continuity plan, a firm should take these five steps:

Step 1: Risk Assessment

This phase includes:

- Evaluation of the company's risks and exposures
- Assessment of the potential impact of various business disruption scenarios
- Determination of the most likely threat scenarios
- Assessment of telecommunication recovery options and communication plans
- Prioritization of findings and development of a roadmap

Step 2: Business Impact Analysis (BIA)

During this phase we collect information on:

- Recovery assumptions, including Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO)
- Critical business processes and workflows as well as the supporting production applications
- Interdependencies, both internal and external
- Critical staff including backups, skill sets, primary and secondary contacts
- Future endeavors that may impact recovery
- Special circumstances

Pro tip: Compiling your BIA into a master list can be helpful from a wholistic standpoint, as well as helpful in identifying pain points throughout the organization.

Step 3: Business Continuity Plan Development

This phase includes:

- Obtaining executive sign-off of Business Impact Analysis
- Synthesizing the Risk Assessment and BIA findings to create an actionable and thorough plan
- Developing department, division and site level plans
- Reviewing plan with key stakeholders to finalize and distribute

Step 4: Strategy and Plan Development

Validate that the recovery times that you have stated in your plan are obtainable and meet the objectives that are stated in the BIA. They should easily be available and readily accessible to staff, especially if and when a disaster were to happen. In the development phase, it's important to incorporate many perspectives from various staff and all departments to help map the overall company feel and organizational focus. Once the plan is developed, we recommend that you have an executive or management team review and sign off on the overall plan.

Step 5: Plan Testing & Maintenance

The final critical element of a business continuity plan is to ensure that it is tested and maintained on a regular basis. This includes:

- Conducting periodic table top and simulation exercises to ensure key stakeholders are comfortable with the plan steps
- Executing bi-annual plan reviews
- Performing annual Business Impact Assessments

QUESTION 427
A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

A. logger

B. Metasploit
C. tcpdump
D. netstat

Correct Answer: D

QUESTION 428
An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

A. SOAP
B. SAML
C. SSO
D. Kerberos

Correct Answer: C

QUESTION 429
A security researching is tracking an adversary by noting its attack and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of intrusion Analysis
B. The Cyber Kill Chain\
C. The MITRE CVE database
D. The incident response process

Correct Answer: A
Explanation:
https://cyware.com/educational-guides/incident-response/what-is-the-diamond-model-of-intrusion-analysis-5f02

QUESTION 430
Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations. Which of the following documents did Ann receive?

A. An annual privacy notice
B. A non-disclosure agreement
C. A privileged-user agreement
D. A memorandum of understanding

Correct Answer: A

QUESTION 431
A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

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

Which of the following MOST likely would have prevented the attacker from learning the service account name?

A. Race condition testing
B. Proper error handling
C. Forward web server logs to a SIEM
D. Input sanitization

Correct Answer: B

QUESTION 432
A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management. Which of the following tools can the analyst use to verify the permissions?

A. ssh
B. chmod
C. 1s
D. setuid
E. nessus
F. nc

Correct Answer: C
Explanation:
https://www.freecodecamp.org/news/the-linux-ls-command-how-to-list-files-in-a-directory-with-options/

QUESTION 433
After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).

A. Disabling guest accounts
B. Disabling service accounts
C. Enabling network sharing
D. Disabling NetBIOS over TCP/IP
E. Storing LAN manager hash values
F. Enabling NTLM

Correct Answer: AD

QUESTION 434