300-215Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Pass Cisco 300-215 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An organization recovered from a recent ransomware outbreak that resulted in significant business damage. Leadership requested a report that identifies the problems that triggered the incident and the security team\\'s approach to address these problems to prevent a reoccurrence. Which components of the incident should an engineer analyze first for this report?

A. impact and flow

B. cause and effect

C. risk and RPN

D. motive and factors

Correct Answer: D

QUESTION 2

```
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong  ag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=X509
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error0D08303A:asn1 encoding routines:asn1_template_noexp_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:536:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=RSA
7369808704:error:04093004:rsa routines:old_rsa_priv_decode:RSA lib:crypto/rsa/rsa_ameth.c:72:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=PKCS8_PRIV_KEY_INFO
7369808704:error:2306F041:PKCS12 routines:PKCS12_key_gen_uni:malloc
failure:crypto/pkcs12/p12_key.c:185:
7369808704:error:2307806B:PKCS12 routines:PKCS12_PBE_keyivgen: key gen
error:crypto/pkcs12/p12_crpt.c:55:
7369808704:error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen
failure:crypto/evp/evp_pbe.c:126:
7369808704:error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit
error:crypto/pkcs12/p12_decr.c:41:
7369808704:error:2306C067:PKCS12 routines:PKCS12_item_i2d_encrypt:encrypt
error:crypto/pkcs12/p12_decr.c:144:
7369808704:error:23073067:PKCS12 routines:PKCS12_pack_p7encdata:encrypt
error:crypto/pkcs12/p12_add.c:119:
```

Refer to the exhibit. What should be determined from this Apache log?

A. A module named mod_ssl is needed to make SSL connections.

B. The private key does not match with the SSL certificate.

C. The certificate file has been maliciously modified

D. The SSL traffic setup is improper

Correct Answer: D

QUESTION 3

```
alert tcp $LOCAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg: "WEB-IIS unicode
directory traversal attempt"; flow:to_server, established; content: "/..%c0%af../";
nocase; classtype:web-application-attack; reference:cve, CVE-2000-0884; threshold:
type limit, track_by_dst, count 1, seconds 60; sid: 981; rev6;)
```

Refer to the exhibit. A company that uses only the Unix platform implemented an intrusion detection system. After the initial configuration, the number of alerts is overwhelming, and an engineer needs to analyze and classify the alerts. The highest number of alerts were generated from the signature shown in the exhibit. Which classification should the engineer assign to this event?

A. True Negative alert

B. False Negative alert

C. False Positive alert

D. True Positive alert

Correct Answer: C

QUESTION 4

What is the function of a disassembler?

A. aids performing static malware analysis

B. aids viewing and changing the running state

C. aids transforming symbolic language into machine code

D. aids defining breakpoints in program execution

Correct Answer: A

Reference: https://scholar.google.co.in/scholar?q=disassembler+aids+performing+static+malware+analysisandhl=enandas_sdt=0andas_vis=1andoi=scholart

QUESTION 5

What is the goal of an incident response plan?

A. to identify critical systems and resources in an organization

B. to ensure systems are in place to prevent an attack

C. to determine security weaknesses and recommend solutions

D. to contain an attack and prevent it from spreading

Correct Answer: D

Reference: https://www.forcepoint.com/cyber-edu/incident-response