are received.

D. The identity of a remote communicating entity and the level of security of the path through which data are received.

Correct Answer: A

QUESTION 303

Which of the following is the most reliable authentication device?

A. Variable callback system.
B. Smart card system.
C. Fixed callback system.
D. Combination of variable and fixed callback system.

Correct Answer: B

QUESTION 304

Which of the following are proprietarily implemented by Cisco?

A. RADIUS+
B. TACACS
C. XTACACS and TACACS+
D. RADIUS

Correct Answer: C

QUESTION 305

What is a protocol used for carrying authentication, authorization, and configuration information between a Network Access Server and a shared Authentication Server?

A. IPSec
B. RADIUS
C. L2TP
D. PPTP

Correct Answer: B

QUESTION 306

RADIUS is defined by which RFC?

A. 2168
B. 2148
C. 2138
D. 2158

Correct Answer: C

QUESTION 307

In a RADIUS architecture, which of the following acts as a client?

A. A network Access Server.
B. None of the choices.
C. The end user.
D. The authentication server.

Correct Answer: A

QUESTION 308

In a RADIUS architecture, which of the following can act as a proxy client?

A. The end user.
B. A Network Access Server.
C. The RADIUS authentication server.
D. None of the choices.

Correct Answer: C

QUESTION 309

Which of the following statements pertaining to RADIUS is incorrect?

A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy
C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes
D. Most RADIUS servers can work with DIAMETER servers.

Correct Answer: D

QUESTION 310
Which of the following is the weakest authentication mechanism?

A. Passphrases
B. Passwords
C. One-time passwords
D. Token devices

Correct Answer: B

QUESTION 311
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various user's accesses.

Correct Answer: C

QUESTION 312
Software generated passwords have what drawbacks?

A. Passwords are not easy to remember.
B. Password are too secure.
C. None of the choices.
D. Passwords are unbreakable.

Correct Answer: A

QUESTION 313
What are the valid types of one time password generator?

A. All of the choices.
B. Transaction synchronous.
C. Synchronous/PIN synchronous.
D. Asynchronous/PIN asynchronous.

Correct Answer: A

QUESTION 314

Which of the following will you consider as most secure?

A. Password
B. One time password
C. Login phrase
D. Login ID

Correct Answer: B

QUESTION 315

What type of password makes use of two totally unrelated words?

A. Login phrase
B. One time password
C. Composition
D. Login ID

Correct Answer: C

QUESTION 316

Which of the following is the correct account policy you should follow?

A. All of the choices.
B. All active accounts must have a password.
C. All active accounts must have a long and complex pass phrase.
D. All inactive accounts must have a password.

Correct Answer: B

QUESTION 317

Which of the following are the advantages of using passphrase?

A. Difficult to crack using brute force.
B. Offers numerous characters.
C. Easier to remember.
D. All of the choices.

Correct Answer: D

QUESTION 318

Which of the following are the correct guidelines of password deployment?

A. Passwords must be masked.
B. All of the choices.
C. Password must have a minimum of 8 characters.
D. Password must contain a mix of both alphabetic and non-alphabetic characters.

Correct Answer: B

QUESTION 319

Why would a 16 characters password not desirable?

A. Hard to remember
B. Offers numerous characters.
C. Difficult to crack using brute force.
D. All of the choices.

Correct Answer: A

QUESTION 320

Which of the following is NOT a good password deployment guideline?

A. Passwords must not be the same as user id or login id.
B. Password aging must be enforced on all systems.
C. Password must be easy to memorize.
D. Passwords must be changed at least once every 60 days, depending on your environment.

Correct Answer: C

QUESTION 321

Rotating password can be restricted by the use of:

A. Password age
B. Password history
C. Complex password
D. All of the choices

Correct Answer: B