Exam Four

In format, the multiple choice questions on Exam Four will resemble those on previous exams. Though, I wouldn't expect a short answer, or a matching, section. In length, expect 60 to 70 multiple choice questions.

The exam will cover materials posted for Module Four including what we have covered in class. That is, it will focus on our Assignments, our Readings and our Lectures. Assignments include:

- Security (Chapter 10) Readings
- Wireless Readings
- Security Videos

Note that each of the above assignments has a specified deliverable. *(In class, I may have misspoken and only mentioned two deliverables.)*
Note also that we are not doing the IoE Reading Assignment deliverable. Though, you are expected to review the IoE Lecture which reviews materials that you read for your New, New Thing Project.

Posted lectures include Wireless, Security, and Internet of Everything (IoE).

You can find assignments and lectures on our Module Four Page at:
http://cis3347.chibana500.com/mod4/

Note One
The Module Four Assignments portfolio is due the same day as Exam Four (25 April).

Note Two
The Learning portfolio is due on Tuesday 9 May at Midnight. Be sure to read the handout concerning the Learning Portfolio at:
http://cis3347.chibana500.com/port/

Study Guide *Module Four V1.1*

Chapter Ten, Network Security

Questions

1. What is the purpose of a disaster recovery plan?
2. Explain how a denial-of-service attack works.
3. What is a firewall?
4. Compare and contrast symmetric and asymmetric encryption.
5. What is PKI? Why is it important?
6. What is a digital certificate?
7. What are the three major ways of authenticating users?

Key Words

1.	confidentiality	refers to the protection of organizational data from unauthorized disclosure of customer and proprietary data.
2.	integrity	the assurance that data have not been altered or destroyed.
3.	risk	a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. (NIST 800-30)
4.	availability	means providing continuous operation of the organization's hardware and software so that staff, customers, and suppliers can be assured of no interruptions in service.
5.	authentication	Quality of having evidence that an entity with which you are interacting are who they claim to be.
6.	brute-force attack	Cryptographic attack where every possible key is tried.
7.	denial-of-service (DoS) attack	Where a network becomes so flooded with messages that it cannot process messages from normal users.
8.	IP spoofing	The creation of Internet Protocol (IP) packets with false source IP addresses, for the purpose of hiding the identity of the sender or impersonating another computing system.
9.	business continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
10.	disaster recovery	Involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
11.	packet-level firewall	Examines the source and destination address of every network packet that passes through it.

Study Guide *Module Four V1.1*

Chapters One, Two, and Five, CCNA Wireless

Each of these chapters includes 'Do I Know This Already?' questions. It would be prudent to know the answers to the following questions:

Chapter One: 1,2,3,4,5,9

Chapter Two: 1,2,4,5,6,7,9,11,12,15

Chapter Five: 1,2,3,4,8,9

Note that the answers are available online in the book's appendix.

Security Video Assignment

Be sure to review the videos at:

http://cis3347.chibana500.com/mod4/SecurityM.html

Specific videos are:

Confidentiality, Integrity, Availability, and Safety (6:11)

Quantitative and Qualitative Risk Assessment (4:31)

Vulnerabilities, Threat Vectors, and Probability (4:26)

Note that each video is accompanied by a written transcript.

Sample Questions

1. Type of encryption that utilizes a pair of different, but related, keys?
   a. Symmetric
   b. Asymmetric
   c. Neo-Classical
   d. Logarithmic Curve

2. Which of the following could be defined as "Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service?"
   a. Vulnerability
   b. Threat
   c. Asset
   d. Risk

3. Which of the following is not one of Porter's smart, connected product's core components?
   A. Physical
   B. 'Smart'
   C. Connectivity
   D. All of the above are core components

4. What kind of model is the Five Forces Model?
    A. Operational
    B. Tactical
    C. **Strategic**
    D. All of the above

5. A transmitter is configured to use a power level of 17 mW. One day it is reconfigured to transmit at a new power level of 34 mW. How much has the power level increased in dB?
    a. 0 dB
    b. 2 dB
    c**. 3 dB**
    d. 17 dB

6. Which one of the following correctly specifies the maximum theoretical data rate of the 802.11b, 802.11a, and 802.11n standards, respectively?
    a**. 11 Mbps, 54 Mbps, 600 Mbps**
    b. 54 Mbps, 54 Mbps, 150 Mbps
    c. 1 Mbps, 11 Mbps, 54 Mbps
    d. 11 Mbps, 20 Mbps, 40 Mbps

Best of luck!
Ed Crowley