You are running a packet sniffer on a network and see a packet containing a long string of "0x90 0x90 0x90 0x90...." in the middle of it traveling to an x86-based machine as a target. This could be indicative of what activity being attempted?

A. Over-subscription of the traffic on a backbone.
B. A source quench packet.
C. A FIN scan.
D. A buffer overflow attack.

Correct Answer: D
Explanation:
A series of the same control characters, hexadecimal code, imbedded in the string is usually an indicator of a buffer overflow attack.

The Intel x86 processors use the hexadecimal number 90 to represent NOP (no operation). Many buffer overflow attacks use long strings of control characters and this is representative of that type of attack.

A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.

Common threats to system availability, integrity, and confidentiality include hardware failure, misuse of system privileges, buffer overflows and other memory attacks, denial of service, reverse engineering, and system hacking.

Since many vulnerabilities result from insecure design and most threats are well known, it is the responsibility of the security architect to ensure that their designs are addressing security requirements appropriately while also ensuring that the system can continue to perform its intended function.

The following answers are incorrect:
Over-subscription of the traffic on a backbone. Is incorrect because if there was Over-subscription of the traffic on a backbone, that would typically result in not being able to send or receive any packets, more commonly known as Denial of Service or DoS.

A source quench packet. This is incorrect because a source quench packet is an ICMP message that contains the internet header plus 64 bits of the original datagram.

A FIN scan. This is incorrect because a FIN scan is when a packet with the FIN flag set is sent to a specific port and the results are then analyzed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 332, for people using the Kindle edition you will find it at Kindle Locations 7310-7315.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Security Architecture and Design (Kindle Locations 1403-1407). . Kindle Edition.

Wikipedia
http://en.wikipedia.org/wiki/Port_scanner
ICMP
http://security.maruhn.com/iptables-tutorial/x1078.html
Wikipedia
http://en.wikipedia.org/wiki/Buffer_overflow

QUESTION 815
What layer of the ISO/OSI model do routers normally operate at?

A. Data link layer
B. Session layer
C. Transport layer
D. Network layer

Correct Answer: D
Explanation:
Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 111).

QUESTION 816
Which of the following is a LAN transmission method?

A. Broadcast
B. Carrier-sense multiple access with collision detection (CSMA/CD)
C. Token ring
D. Fiber Distributed Data Interface (FDDI)

Correct Answer: A
Explanation:
LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.

CSMA/CD is a common LAN media access method.
Token ring is a LAN Topology.
LAN transmission protocols are the rules for communicating between computers on a LAN. Common LAN transmission protocols are: polling and token-passing. A LAN topology defines the manner in which the network devices are organized to facilitate communications.
Common LAN topologies are: bus, ring, star or meshed.

LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.
LAN media access methods control the use of a network (physical and data link layers).
They can be Ethernet, ARCnet, Token ring and FDDI.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 103).

HERE IS A NICE OVERVIEW FROM CISCO:

LAN Transmission Methods
LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.

LAN Topologies
LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks--including 100BaseT--implement a bus topology

Sources: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introlan.htm

QUESTION 817
What type of cable is used with 100Base-TX Fast Ethernet?

A. Fiber-optic cable
B. Category 3 or 4 unshielded twisted-pair (UTP).
C. Category 5 unshielded twisted-pair (UTP).
D. RG-58 cable.

Correct Answer: C
Explanation:
This is the type of cabling recommended for 100Base-TX networks.
Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling.
"Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for 100Mbps operation.
RG-58 cable is incorrect. Incorrect media type for 100Base-TX.
References:
CBK, p. 428
AIO3, p. 455

QUESTION 818
How do you distinguish between a bridge and a router?

A. A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.
B. "Bridge" and "router" are synonyms for equipment used to join two networks.
C. The bridge is a specific type of router used to connect a LAN to the global Internet.
D. The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Correct Answer: D
Explanation:
A bridge operates at the Data Link Layer and a router operates at the Network Layer.

The following answers are incorrect:

A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to. Is incorrect because both forward packets this is not distinctive enough.

"Bridge" and "router" are synonyms for equipment used to join two networks. Is incorrect because the two are unique and operate at different layers of the OSI model.

The bridge is a specific type of router used to connect a LAN to the global Internet. Is incorrect because a bridge does not connect a LAN to the global internet, but connects networks together creating a LAN.

QUESTION 819
Packet Filtering Firewalls can also enable access for:

A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.

Correct Answer: A
Explanation:
Firewall rules can be used to enable access for traffic to specific ports or services. "Service numbers" is rather stilted English but you may encounter these types of wordings on the actual exam -- don't let them confuse you.

"Only unauthorized application port or service numbers" is incorrect. Unauthorized ports/services would be blocked in a properly installed firewall rather than permitting access.

"Only authorized application port or ex-service numbers" is incorrect. "Ex-service" numbers is a nonsense term meant to distract you.

"Only authorized application port or service integers." While service numbers are in fact integers, the more usual (and therefore better) answer is either service or "service number."

References:
CBK, p. 464
AIO3, pp. 482 ?484

QUESTION 820
What is called the access protection system that limits connections by calling back the number of a previously authorized location?

A. Sendback systems
B. Callback forward systems
C. Callback systems
D. Sendback forward systems

Correct Answer: C
Explanation:
The Correct Answer: Call back Systems; Callback systems provide access protection by calling back the number of a previously authorized location, but this control can be compromised by call forwarding.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 821
Which of the following is a tool often used to reduce the risk to a local area network (LAN) that has external connections by filtering Ingress and Egress traffic?

A. a firewall.
B. dial-up.
C. passwords.
D. fiber optics.

Correct Answer: A
Explanation:
The use of a firewall is a requirement to protect a local area network (LAN) that has external connections without that you have no real protection from fraudsters.

The following answers are incorrect:

dial-up. This is incorrect because this offers little protection once the connection has been established.

passwords. This is incorrect because there are tools to crack passwords and once a user has been authenticated and connects to the external connections, passwords do not offer protection against incoming TCP packets.

fiber optics. This is incorrect because this offers no protection from the external connection.

QUESTION 822
What is the main characteristic of a bastion host?

A. It is located on the internal network.
B. It is a hardened computer implementation
C. It is a firewall.
D. It does packet filtering.
Correct Answer: B
Explanation: