Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 5267-5268). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Internet_protocol_suite

QUESTION 831
Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?

A. DHCP
B. BootP
C. DNS
D. ARP

Correct Answer: B
Explanation:
BootP was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN. Over time, it has expanded to allow centralized configuration of many aspects of a host's identity and behavior on the network. Note that DHCP, more complex, has replaced BootP over time.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

QUESTION 832
Secure Shell (SSH-2) supports authentication, compression, confidentiality, and integrity, SSH is commonly used as a secure alternative to all of the following protocols below except:

A. telnet
B. rlogin
C. RSH
D. HTTPS

Correct Answer: D
Explanation:
HTTPS is used for secure web transactions and is not commonly replaced by SSH.
Users often want to log on to a remote computer. Unfortunately, most early implementations to meet that need were designed for a trusted network. Protocols/programs, such as TELNET, RSH, and rlogin, transmit unencrypted over the network, which allows traffic to be easily intercepted. Secure shell (SSH) was designed as an alternative to the above insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel. The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates. Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.

The following were wrong answers:

telnet is an incorrect choice. SSH is commonly used as an more secure alternative to telnet. In fact Telnet should not longer be used today. rlogin is and incorrect choice. SSH is commonly

used as a more secure alternative to rlogin.
RSH is an incorrect choice. SSH is commonly used as a more secure alternative to RSH.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7077-7088). Auerbach Publications. Kindle Edition.

QUESTION 833
Upon which of the following ISO/OSI layers does network address translation operate?

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

Correct Answer: D
Explanation:
Network address translation (NAT) is concerned with IP address translation between two networks and operates at the network layer (layer 3).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 3: Telecommunications and Network Security (page 440).

QUESTION 834
Which of the following protocols is not implemented at the Internet layer of the TCP/IP protocol model?

A.   User datagram protocol (UDP)
B.   Internet protocol (IP)
C.   Internet Group Management Protocol (IGMP)
D.   Internet control message protocol (ICMP)
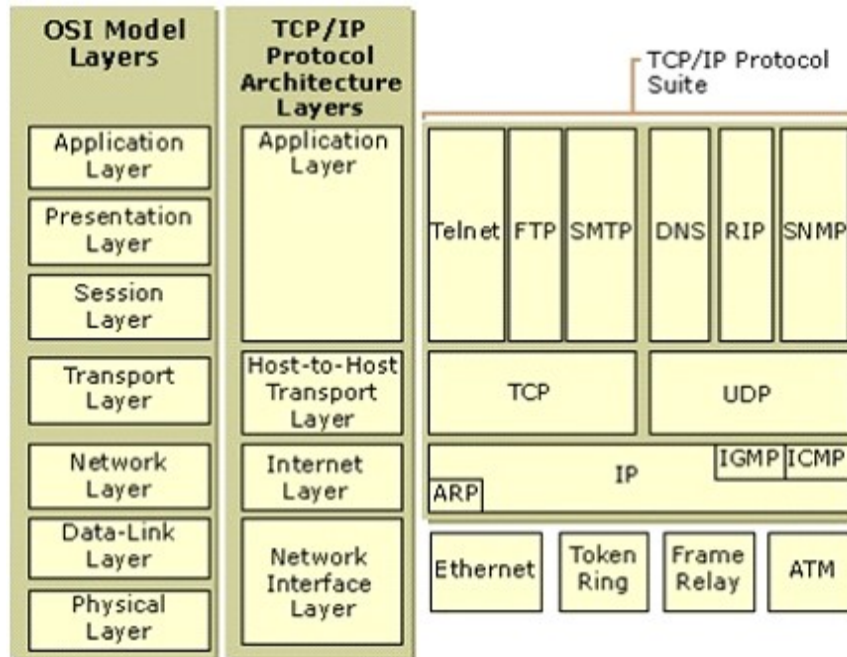
Correct Answer: A
Explanation:
The User Datagram Protocol (UDP) is implemented at the host-to-host transport layer, not at the internet layer.

Protocol at what layer?
Ensure you are familiar with both the OSI model and the DoD TCP/IP model as well. You need to know how to contrast the two side by side and what are the names being used on both side.
Below you have a graphic showing the two and how things maps between the two as well as some of the most common protcolos found at each of the layers:
Protocols at what layers of the DoD TCP/IP model

Graphic from http://technet.microsoft.com/en-us/library/cc958821.aspx

The following are incorrect answers:
All of the other protocols sit at the Internet Layer of the TCP/IP model.

NOTE:
Some reference are calling the Transport layer on the DoD model Host-to-Host.

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO), 6th edition , Telecommunication and Network Security, Page 518,534
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 85).
Microsoft Technet at http://technet.microsoft.com/en-us/library/cc958821.aspx

QUESTION 835
Which of the following remote access authentication systems is the most robust?

A. TACACS+
B. RADIUS
C. PAP
D. TACACS

Correct Answer: A
Explanation:
TACACS+ is a proprietary Cisco enhancement to TACACS and is more robust than RADIUS.
PAP is not a remote access authentication system but a remote node security protocol.
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 122).

QUESTION 836
Which of the following is the primary reason why a user would choose a dial-up modem connection to the Internet when they have a faster, secure Internet connection through the organization's network?

A.   To access web sites that blocked by the organization's proxy server.
B.   To set up public services using the organization's resources.
C.   To check their personal e-mail.
D.   To circumvent the organization's security policy.

Correct Answer: D
Explanation:
All the choices above represent examples of circumventing the organization's security policy, which is the primary reason why a user would be using a dial-up Internet connection when a secure connection is available through the organization's network.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

QUESTION 837
Which xDSL flavour delivers both downstream and upstream speeds of 1.544 Mbps over two copper twisted pairs?

A.   HDSL
B.   SDSL
C.   ADSL
D.   VDSL

Correct Answer: A
Explanation:
High-rate Digital Subscriber Line (HDSL) delivers 1.544 Mbps of bandwidth each way over two copper twisted pairs. SDSL also delivers 1.544 Mbps but over a single copper twisted pair. ADSL and VDSL offer a higher bandwidth downstream than upstream.
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 115).

QUESTION 838
Which of the following media is MOST resistant to tapping?

A.   microwave.
B.   twisted pair.
C.   coaxial cable.
D.   fiber optic.

Correct Answer: D
Explanation:
Fiber Optic is the most resistant to tapping because Fiber Optic uses a light to transmit the signal. While there are some technologies that will allow to monitor the line passively, it is very difficult to tap into without detection sot this technology would be the MOST resistent to tapping.

The following answers are in correct:

microwave. Is incorrect because microwave transmissions can be intercepted if in the path of the broadcast without detection.
twisted pair. Is incorrect because it is easy to tap into a twisted pair line.
coaxial cable. Is incorrect because it is easy to tap into a coaxial cable line.

QUESTION 839
Which type of attack involves impersonating a user or a system?

A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack

Correct Answer: B
Explanation:
A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.
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 77).

QUESTION 840
What is the main difference between a Smurf and a Fraggle attack?

A.   A Smurf attack is ICMP-based and a Fraggle attack is UDP-based.
B.   A Smurf attack is UDP-based and a Fraggle attack is TCP-based.
C.   Smurf attack packets cannot be spoofed.
D.   A Smurf attack is UDP-based and a Fraggle attack is ICMP-based.

Correct Answer: A
Explanation:
Fraggle is an attack similar to Smurf, but instead of using ICMP, it uses UDP.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 11: Application and System Development (page 790).

QUESTION 841
Which of the following NAT firewall translation modes offers no protection from hacking attacks to an internal host using this functionality?

A. Network redundancy translation
B. Load balancing translation
C. Dynamic translation
D. Static translation

Correct Answer: D
Explanation:
Static translation (also called port forwarding), assigns a fixed address to a specific internal network resource (usually a server).