SE 4C03 Winter 2007

Final Examination Answer Key

Instructor: William M. Farmer

Revised: 21 April 2007

(1) [2 pts.] The tcpdump program is not designed to collect the UDP datagrams that arrive at a network interface. Is this statement true or false?

A.) True.

B.) [✓ False.]

(2) [2 pts.] All attachments to e-mail messages that are transferred by SMTP must be encoded as ASCII text. Is this statement true or false?

A.) [✓ True.]

B.) False.

(3) [2 pts.] Some hosts running TCP/IP do not have domain names assigned to them. Is this statement true or false?

A.) [✓ True.]

B.) False.

(4) [2 pts.] It is easier to spoof a domain name than a source address. Is this statement true or false?

A.) [✓ True.]

B.) False.

(5) [2 pts.] A bastion host is a computer that is not connected to any SPN. Is this statement true or false?

A.) True.

B.) [✓ False.]

(6) [2 pts.] Key distribution is a major concern for conventional encryption but not for public key encryption. Is this statement true or false?

A.) True.

B.) [✓ False.]

(7) [2 pts.] An Ethernet network interface card is physically prevented from accepting any Ethernet frame whose destination address is not identical to the card's Ethernet address. Is this statement true or false?

A.) True.

B.) [✓ False.]

(8) [2 pts.] An IP datagram traveling across the Internet can undergo fragmentation more than once and reassembly at most once. Is this statement true or false?

A.) [✓ True.]

B.) False.

(9) [2 pts.] An Ethernet hub is a kind of packet router. Is this statement true or false?

A.) True.

B.) [✓ False.]

(10) [2 pts.] The purpose of the `inetd` server is to listen for requests on behalf of other network servers. Is this statement true or false?

A.) [✓ True.]

B.) False.

(11) [2 pts.] The `traceroute` program and `ping` program with the record route option use different mechanisms to record the route to the destination IP address.

A.) [✓ True.]

B.) False.

(12) [2 pts.] TCP is a delivery service that is both reliable and secure. Is this statement true or false?

A.) True.

B.) [✓ False.]

(13) [2 pts.] The Bell-LaPadula security model is concerned with reading and writing documents at different security levels. Is this statement true or false?

A.) [✓ True.]

B.) False.

(14) [2 pts.] A security posture is to a security policy as a requirements specification is to an implementation. Is this statement true or false?

A.) True.

B.) [✓ False.]

(15) [2 pts.] The process that handles the `ping` service listens at

A.) A reserved port.

B.) An ephemeral port.

C.) Port 17.

D.) [✓ No port at all.]

(16) [2 pts.] The original backbone of the Internet was the

A.) [✓ ARPANET.]

B.) MILNET.

C.) NIPRNET.

D.) NSFNET.

(17) [2 pts.] Someone who wants to break into a host will often use port scanning to find

A.) Which ports are currently in use.

B.) All the host's open TCP connections.

C.) The best place to install a virus.

D.) [✓ Network servers that could be exploited.]

(18) [2 pts.] A side channel attack on an algorithm is an attack on

A.) The author of the algorithm.

B.) [✓ An implementation of the algorithm.]

C.) The communication channels of the algorithm.

D.) The algorithm itself.

(19) [2 pts.] When a user is running X Windows on a computer C,

A.) The X Windows server and its clients must be running on C.

B.) The X Windows clients must be running on C, but the X Windows server may be running on a computer different from C.

C.) The X Windows server must be running on C, and the X Windows clients must be running on computers different from C.

D.) [✓ The X Windows server must be running on C, and the X Windows clients may be running on C or on computers different from C.]

(20) [2 pts.] Suppose host A has sent an IP datagram encapsulating a TCP segment to host B over the Internet and a router R along the way drops the IP datagram due to congestion. What will R normally do after dropping the datagram.

A.) Send a quench source TCP message to A.

B.) Send a no acknowledgment TCP message to B.

C.) [✓ Send an ICMP message to A.]

D.) Send an ICMP message to both A and B.

(21) [2 pts.] Which network service uses UDP?

A.) DNS.

B.) RIP.

C.) TFTP.

D.) [✓ All of the above.]

(22) [2 pts.] Which organization is in charge of managing IP addresses and DNS domain names?

A.) [✓ ICANN.]

B.) IETF.

C.) ISO.

D.) ISOC.

(23) [2 pts.] Which directory is intended for files that can grow arbitrarily large?

A.) `/bin`.

B.) `/dev`.

C.) `/etc`.

D.) [✓ `/var`.]

(24) [2 pts.] A single lost TCP segment will cause ______________ TCP segment(s) to be retransmitted.

A.) Exactly one.

B.) At most one.

C.) [✓ At least one.]

D.) Any number of.

(25) [2 pts.] Which application encapsulates IP datagrams in other IP datagrams.

A.) Arkansas cryptotalk.

B.) GGP.

C.) SSH.

D.) [✓ VPN.]

(26) [2 pts.] Today most FTP servers operate in

A.) Normal mode with a single TCP connection.

B.) Passive mode with a single TCP connection.

C.) Normal mode with multiple TCP connections.

D.) [✓ Passive mode with multiple TCP connections.]

(27) [2 pts.] SSH uses public key encryption to

A.) [✓ Exchange session keys.]

B.) Encrypt the SSH session.

C.) Authenticate the client process.

D.) All of the above.

(28) [2 pts.] Which of the following can be done by both conventional and public encryption?

A.) [✓ Data encryption.]

B.) Digital signing.

C.) Cryptographic hashing.

D.) Non-repudiation.

(29) [2 pts.] Which routing protocol uses neither vector-distance nor link-state routing?

A.) [✓ BGP.]

B.) GGP.

C.) HELLO.

D.) RIP.

(30) [2 pts.] Which conventional encryption algorithm is no longer considered secure enough for many applications?

A.) AES.

B.) Blowfish.

C.) [✓ DES.]

D.) IDEA.

(31) [2 pts.] Which TCP-based network service cannot be adequately handled by normal packet filtering?

A.) [✓ FTP.]

B.) HTTP.

C.) SSH.

D.) Telnet.

(32) [2 pts.] Which kind of server provides files to a client process without usually authenticating the user of the client process?

A.) Anonymous FTP.

B.) HTTP.

C.) TFTP.

D.) [✓ All of the above.]

(33) [2 pts.] Which routing protocol does not measure the distance of a route as the number of hops?

A.) GGP.

[✓ B.) HELLO.]

C.) OSPF.

D.) RIP.

(34) [2 pts.] A portmapper is a program that

A.) Assigns ports to servers.

[✓ B.) Forwards requests to servers that are not listening at a standard port.]

C.) Looks for ports at which other servers are listening.

D.) All of the above.

(35) [2 pts.] Which means of probing a network can be thwarted by filtering out all ICMP traffic?

A.) DNS.

B.) `ping`.

C.) `traceroute`.

[✓ D.) All of the above.]

(36) Consider a subnet whose subnet address is 78.192.126.32 and whose (unconventional) mask is 255.240.255.96.

A.) [5 pts.] How many IP addresses are contained in this subnet?

Answer: $2^{4+6} = 2^{10}$.

B.) [5 pts.] What are the lowest and highest addresses in this subnet?

Answer: 78.192.126.32, 78.207.126.191.

C.) [5 pts.] How many class A, B, and C networks intersect this subnet? List the network addresses of these class networks.

Answer: 1 class A network with network address 78.0.0.0 intersects this subnet.

(37) [15 pts.] Below is a diagram of a conventional internet using the TCP/IP protocols (which is not shown).

$\mathsf{H}_1, \ldots, \mathsf{H}_3$ are hosts. $\mathsf{I}_1, \ldots, \mathsf{I}_6$ are interfaces to the single physical networks $\mathsf{SPN}_1, \ldots, \mathsf{SPN}_3$ and the Internet. $\mathsf{J}_1, \ldots, \mathsf{J}_3$ are interfaces to loopback networks. There are other hosts and interfaces that are not shown. The following table shows what IP addresses and subnet masks are assigned to the $\mathsf{I}_1, \ldots, \mathsf{I}_6$ interfaces.

Interface	**IP Address**	**Subnet Mask**
I_1	215.206.89.146	255.255.255.248
I_2	215.206.89.155	255.255.255.248
I_3	215.206.89.156	255.255.255.248
I_4	215.206.89.162	255.255.255.248
I_5	215.206.89.165	255.255.255.248
I_6	249.56.145.98	255.255.255.0

Recall that a route in a subnet routing table has the form (a, m, r, i) where:

- a is the address of a subnet S.
- m is the mask of S.
- r is an IP address for the "next hop" ($r = *$ for direct routes).
- i is an interface.

Write down the routing table for H_2 as a list of (a, m, r, i) tuples with the smallest possible number of indirect routes. You may use a default route but no host-specific routes.

Answer:

(127.0.0.0,	255.0.0.0,	$*$,	J_2)
(215.206.89.152,	255.255.255.248,	$*$,	I_3)
(215.206.89.160,	255.255.255.248,	$*$,	I_4)
(215.206.89.144,	255.255.255.248,	215.206.89.155,	I_3)
(0.0.0.0,	0.0.0.0,	215.206.89.165,	I_4)