SE 4C03 Winter 2003

Final Examination Answer Key

Instructor: William M. Farmer

(1) [2 pts.] Both the source and destination IP addresses are used to route IP datagrams. Is this statement true or false?

A.) True.

B.) [False.]

(2) [2 pts.] IP datagrams, encapsulated in Ethernet frames, are the only messages sent across the Ethernet networks of the Little Internet. Is this statement true or false?

A.) True.

B.) [False.]

(3) [2 pts.] Trying out all possible keys would not be a feasible method for discovering the key used for a shuffle cipher. Is this statement true or false?

A.) [True.]

B.) False.

(4) [2 pts.] TFTP servers and anonymous FTP servers expose a host to essentially the same dangers. Is this statement true or false?

A.) [True.]

B.) False.

(5) [2 pts.] TCP segments are sometimes encapsulated directly in physical network frames. Is this statement true or false?

A.) [True.]

B.) False.

(6) [2 pts.] SUID programs should never be used on a computer running Unix. Is this statement true or false?

A.) True.

B.) [False.]

(7) [2 pts.] A DNS domain name maps to a unique IP address. Is this statement true or false?

A.) True.

B.) **False.**

(8) [2 pts.] If an IP datagram is too large to fit in the data area of a maximum size frame for a SPN, the IP datagram will be fragmented before crossing the SPN and then reassembled after crossing the SPN. Is this statement true or false?

A.) True.

B.) **False.**

(9) [2 pts.] On a computer running Unix or Linux, the `inetd` server is a "metaserver" that manages all other servers on the computer. Is this statement true or false?

A.) True.

B.) **False.**

(10) [2 pts.] Most applications of encryption on the Internet utilize

A.) Conventional encryption.

B.) Public key encryption.

C.) **Both conventional and public key encryption.**

D.) Key distribution centers.

(11) [2 pts.] IP forwarding is turned on in approximately _____ running TCP/IP.

A.) 50% of hosts with exactly one physical network interface.

B.) 95% of hosts with exactly one physical network interface.

C.) 50% of hosts with more than one physical network interface.

D.) **95% of hosts with more than one physical network interface.**

(12) [2 pts.] The HTTP protocol can allow a client to

A.) Get a file stored on the server's host.

B.) Store a file on the server's host.

C.) Execute a program stored on the server's host.

D.) **All of the above.**

(13) [2 pts.] What would be a better name for `tcpdump`?

A.) `framedump.`

B.) `ipdump`.

C.) `ethernetdump`.

D.) `udpdump`.

(14) [2 pts.] The `traceroute` program uses _____ to find the route to a destination host.

A.) Telnet connection requests.

B.) TCP acknowledgments.

C.) The ICMP ping service.

D.) ICMP "time exceeded" messages.

(15) [2 pts.] Which of the following network technologies is best for real-time video transmission?

A.) FDDI.

B.) Ethernet.

C.) Infrared.

D.) ATM.

(16) [2 pts.] How many reserved protocol ports does a computer running TCP/IP have?

A.) 2^8.

B.) 2^{10}.

C.) 2^{11}.

D.) 2^{16}.

(17) [2 pts.] Suppose C is an X Windows client that is started from an SSH shell. The destination port of TCP packets sent from C to the X Windows server will normally be

A.) 22.

B.) 23.

C.) 6000.

D.) 6001.

(18) [2 pts.] Which of the following defense mechanisms can effectively protect an FTP server?

A.) The FTP passive operation mode.

B.) A circuit-level proxy server.

C.) A stateless packet filter.

D.) All of the above.

(19) [2 pts.] Suppose that an IP datagram with destination IP address d is being forwarded by a host. What happens if d does not match any entry in the host's routing table.

A.) An ICMP "network unreachable" message is sent back to the source address of the IP datagram.

B.) The IP datagram is sent back to the source address of the IP datagram.

C.) A "request for route" is broadcasted to each SPN directly connected to the host.

D.) All of the above.

(20) [2 pts.] A UDP-based application protocol often provides

A.) Some reliability.

B.) Support for stream delivery.

C.) Support for virtual circuits.

D.) Session encryption.

(21) [2 pts.] What is usually returned when a request is made to connect to a TCP port at which no server is listening?

A.) A TCP segment with the `ACK` and `RST` bits set to 1.

B.) A TCP segment with the `ACK` and `SYN` bits set to 1.

C.) A TCP segment with the `ACK` and `FIN` bits set to 1.

D.) An ICMP "host unreachable" message.

(22) [2 pts.] Which of the following entities "resides" in Platonic heaven?

A.) TCP circuits.

B.) Protocol ports.

C.) The loopback network.

D.) All of the above.

(23) [2 pts.] Ordinarily, a packet filter accepts or denies an IP datagram on the basis of information in

A.) The header of the IP datagram.

B.) The header and data area of the IP datagram

C.) The headers of the IP datagram and encapsulated UDP or TCP packet.

D.) The header of the encapsulated UDP or TCP packet.

(24) [4 pts.] What is the difference between an Ethernet hub and an Ethernet switch?

Answer: An Ethernet hub multiplies and forwards Ethernet frames as *electronic signals*; a hub knows nothing about the informational content of the frame and thus forwards all frames it receives. An Ethernet switch multiplies and forwards Ethernet frames as *digital packets*; a switch can use the informational content of the frame to selectively forward the frames its receives.

(25) [4 pts.] For SSH with public key authentication, what is the purpose of the passphrase?

Answer: The passphrase is used to decrypt the user's private key.

(26) [4 pts.] What is a public key certificate?

Answer: A public key certificate is a document digitally signed by a public key authority that contains the name of a subject and a public key for the subject.

(27) [4 pts.] Why must the encrypted passwords for user accounts be strongly protected?

Answer: The password corresponding to its encrypted form can be discovered from the encrypted form by a brute force attack, especially if the password is short, a word in a dictionary, or easily derivable from a word in a dictionary.

(28) [4 pts.] Compute the network address of the class network that contains the IP address 207.34.45.244.

Answer: 207.34.45.0.

(29) [4 pts.] Write the `iptables` command to filter out incoming TCP packets whose source address is the address of the loopback interface.

Answer: `iptables -A INPUT -p tcp -s 127.0.0.1 -j DROP`

(30) [4 pts.] Using circles for SPNs, boxes for hosts, and lines for interfaces, draw a bipartite graph that represents an internet that satisfies the following properties:

A.) There are two SPNs in the internet.

B.) Each SPN is connected to exactly 5 hosts.

C.) There is exactly one internet router in the internet.

Answer: Not shown.

(31) [4 pts.] Suppose that you have an account on a computer running an SSH server that only allows public key authentication. What would have to be done to enable some user U to log from their account into your account with SSH?

Answer: A copy of U's SSH public key would have to be put in your account's authorized keys file.

(32) [6 pts.] Consider the subnet whose address is 154.68.0.0. and whose mask is 255.207.0.0.

A.) How many IP addresses are members of this subnet?

Answer: 2^{18}.

B.) How many class B networks are subsets of this subnet?

Answer: $2^2 = 4$.

(33) [6 pts.] Complete the following table which correlates kinds of data protection with Unix file permissions:

Kind of Data Protection	**Unix File Permission**
Privacy	**r**
Integrity	`w`
Availability	`x`

(34) [10 pts.] Suppose that a host H running TCP/IP has the loopback interface `lo` and the following two physical network interfaces:

Interface	**IP Address**	**Subnet Mask**
`eth0`	200.103.14.123	255.255.255.240
`eth1`	200.103.16.99	255.255.255.240

The `eth0` interface is on an Ethernet network such that every host on the network, except for H, has exactly one physical network interface. The `eth1` interface is connected by an Ethernet crossover cable to an interface with IP address 200.103.16.98.

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 in S for the "next hop" ($r = *$ for direct routes).
- i is an interface.

Write down the routing table for H as a list of (a, m, r, i) tuples. Do not use any host-specific routes, and keep the number of indirect routes as small as possible.

Answer:

(127.0.0.0,	255.0.0.0,	$*$,	`lo`)
(200.103.14.112,	255.255.255.240,	$*$,	`eth0`)
(200.103.16.96,	255.255.255.240,	$*$,	`eth1`)
(0.0.0.0,	0.0.0.0,	200.103.16.98,	`eth1`)