SE 4C03 Winter 2006

Final Examination Answer Key

Instructor: William M. Farmer

(1) [2 pts.] A misconfigured anonymous FTP server can be as dangerous as an TFTP server.

(a) [True.]
(b) False.

(2) [2 pts.] A session key is usually a conventional secret key. Is this statement true or false?

(a) [True.]
(b) False.

(3) [2 pts.] A network server always listens at a reserved UDP or TCP port. Is this statement true or false?

(a) True.
(b) [False.]

(4) [2 pts.] Every organization needs a security policy. Is this statement true or false?

(a) [True.]
(b) False.

(5) [2 pts.] A fragmented IP datagram traveling across the Internet can undergo reassembly more than once. Is this statement true or false?

(a) True.
(b) [False.]

(6) [2 pts.] The Java programming language can be used to create TCP-based communication channels between processes. Is this statement true or false?

(a) [True.]
(b) False.

(7) [2 pts.] To protect an FTP server from attack, most FTP servers today operate in normal mode. Is this statement true or false?

(a) True.
(b) [False.]

(8) [2 pts.] Mail sent using SMTP normally crosses the Internet by making several hops from one mail server to another. Is this statement true or false?

(a) True.
(b) [False.]

(9) [2 pts.] A DNS root server can answer any DNS question. Is this statement true or false?

(a) True.
(b) [False.]

(10) [2 pts.] There is no advantage to having several stateless packet filters on the same host. Is this statement true or false?

(a) True.
(b) [False.]

(11) [2 pts.] To display a web browser running on a remote host on your local host as an X Window you must start up an X Windows server on the remote host. Is this statement true or false?

(a) True.
(b) [False.]

(12) [2 pts.] Even a correctly configured SUID program is quite dangerous. Is this statement true or false?

(a) True.
(b) [False.]

(13) [2 pts.] Passwords are protected using

(a) Secret key encryption.
(b) Public key encryption.
(c) [One-way encryption.]
(d) Two-way encryption.

(14) [2 pts.] Which TCP code bit means that a given sequence of octets should be processed out of order?

(a) `RST`.
(b) `PSH`.
(c) [`URG`.]
(d) `FIN`.

(15) [2 pts.] The Routing Information Protocol (RIP) is dangerous because

(a) It is based on ICMP.
(b) It does not include authentication.
(c) It employs a weak encryption algorithm.
(d) It sends passwords as plaintext.

(16) [2 pts.] A pseudorandom number generator is a computer program that

(a) Is deterministic.
(b) Is periodic.
(c) Produces numbers that are "approximately" random.
(d) All of the above.

(17) [2 pts.] A collection of proxy servers for incoming network requests _____ a stateless packet filter.

(a) Provides a better firewall than.
(b) Complements.
(c) Has faster throughput than.
(d) All of the above.

(18) [2 pts.] _____ does not involve secret keys.

(a) Conventional encryption.
(b) Public key encryption.
(c) Cryptographic hashing.
(d) The RSA algorithm.

(19) [2 pts.] Several TCP connections are used simultaneously in a session of the _____ network service.

(a) DNS.
(b) HTTP.
(c) SMTP.
(d) FTP.

(20) [2 pts.] The purpose of port scanning a host is to

(a) Disable the host with a SYN flood.
(b) Find all the host's open TCP connections.
(c) Determine which servers are listening for requests on the host.
(d) Look for hidden viruses.

(21) [2 pts.] Public key encryption is used the least for

(a) Message encryption.

(b) Secret key distribution.

(c) Digital signatures.

(d) Integrity verification.

(22) [2 pts.] If it is possible for you to use rlogin on host A to log into account X on host B without a password, then

(a) It is possible for any superuser on A to log into X.

(b) It is possible for any user on A to log into X.

(c) It is possible for you to log into host A without a password.

(d) All of the above.

(23) [2 pts.] Which network service could you use to find a port on a remote host at which a particular network server is listening?

(a) Portmapper.

(b) Portscanner.

(c) Find.

(d) Gopher.

(24) [2 pts.] Which kind of network server can be a "poor man's" web server?

(a) Telnet.

(b) FTP.

(c) SMTP.

(d) HTML.

(25) [2 pts.] Secure Shell

(a) Uses just convention encryption.

(b) Uses just public key encryption.

(c) Uses both conventional and public key encryption.

(d) Uses neither conventional nor public key encryption.

(26) [2 pts.] Which of the following would normally not be considered a firewall?

(a) A router running a packet filter.

(b) A host running a series of proxy servers.

(c) A screened subnet of bastion hosts.

(d) A host running a web server.

(27) [2 pts.] Public key encryption is used in SSH for authentication and

(a) File access control.

(b) Data privacy.

(c) Data integrity.

(d) Session key distribution.

(28) [2 pts.] Which communication protocol is not suitable for a network service based on the client-server model.

(a) ICMP.

(b) UDP.

(c) TCP.

(d) All of the above.

(29) [4 pts.] Why is FTP more difficult for firewalls to handle than most other common network services.

Answer: An FTP session involves the use of several simultaneous TCP connections, namely, one control connection and one or more data connections. In order for a firewall to adequately handle FTP traffic, the firewall must keep track of the set of control and data connections that comprise each FTP session. Not all firewalls have the capability to do this, e.g., firewalls based on stateless packet filters.

(30) [4 pts.] What is the purpose of the `inetd` server?

Answer: The `inetd` server listens for connection requests on behalf of other network servers. When `inetd` receives a request on port p, it invokes the server bound to p and hands the server the request. Thus the network servers handled by `inetd` run only when they are needed.

(31) [4 pts.] Give an example of server that does not listen at a UDP or TCP port.

Answer: `tcpd`, the TCP wrapper.

(32) Consider a subnet whose subnet address is 30.245.181.187 and whose (unconventional) mask is 255.255.120.128.

(a) [4 pts.] What are the lowest and highest addresses in this subnet?

Answer: 30.245.48.128, 30.245.183.255

(b) [4 pts.] How many IP addresses are contained in this subnet?

Answer: $2^{4+7} = 2^{11}$.

(33) Consider the IP address 130.140.150.160.

(a) [4 pts.] Write this address in binary (base 2).

Answer: 10000010.10001100.10010110.10100000

(b) [4 pts.] Write this address in hexidecimal (base 16).

Answer: 82.8C.96.A0

(c) [4 pts.] What is the network address of the class network that contains this address?

Answer: 130.140.0.0

(34) [12 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	213.251.34.177	255.255.255.224
I_2	213.251.35.165	255.255.255.240
I_3	213.251.35.166	255.255.255.240
I_4	213.251.35.180	255.255.255.240
I_5	213.251.35.185	255.255.255.240
I_6	75.213.45.52	255.255.0.0

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_1 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_1)
(213.251.34.160,	255.255.255.224,	$*$,	I_1)
(213.251.35.160,	255.255.255.240,	$*$,	I_2)
(0.0.0.0,	0.0.0.0,	213.251.35.166,	I_2)