Software Engineering 4C03
Answer Key

DAY CLASS — Dr. William M. Farmer
DURATION OF EXAMINATION: 2 Hours
MCMASTER UNIVERSITY FINAL EXAMINATION — April 2002

(1) [2 pts.] Conventional encryption cannot be used to digitally sign public documents. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(2) [2 pts.] Every host running TCP/IP needs to have IP forwarding turned on. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(3) [2 pts.] Suppose A and B are two hosts on the Little Internet that are not on the same SPN. Suppose further that the IP Network Security Policy of Lab Exercise 5 is implemented by every host in the Little Internet. Then it would be impossible for a user on A to log into B using SSH (either directly or indirectly). Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(4) [2 pts.] The purpose of the exterior gateway protocol BGP is to exchange routes between autonomous systems. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(5) [2 pts.] When an IP datagram is transferred from host A to host B, fragmentation of the datagram may occur at most once. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

Continued on page 2

(6) [2 pts.] A Web browser can request HTML documents from an FTP server. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(7) [2 pts.] Every socket is associated with both a protocol port and an IP address. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(8) [2 pts.] A router using a vector-distance protocol will normally send large amounts of information to a small number of routers. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(9) [2 pts.] ICMP can be used to

A.) Request the subnet mask of an SPN.

B.) Tell a host to change a route in its routing table.

C.) "Ping" a host.

D.) $\boxed{\text{All of the above.}}$

(10) [2 pts.] A packet filtering firewall can be used to

A.) Allow TCP connections to the Internet to be initiated from inside but not from outside the firewall.

B.) Allow an FTP client inside the firewall to access a normal mode FTP server outside the firewall without exposing the client's host to attack.

C.) Allow an FTP client outside the firewall to access a passive mode FTP server inside the firewall without exposing the server's host to attack.

D.) All of the above.

(11) [2 pts.] Which TCP code bit will usually be set when sending a command from a telnet client to a telnet server?

A.) URG.

B.) $\boxed{\text{PSH.}}$

C.) RST.

D.) SYN.

Continued on page 3

(12) [2 pts.] The loopback address is a member of a

A.) $\boxed{\text{Class A network.}}$
B.) Class B network.
C.) Class C network.
D.) None of the above.

(13) [2 pts.] Which protocol might be used by a hacker to direct packets to a wrong destination host?

A.) ARP.
B.) ICMP.
C.) RIP.
D.) $\boxed{\text{All of the above.}}$

(14) [2 pts.] Which of the following encryption algorithms is appropriate for link encryption?

A.) $\boxed{\text{DES.}}$
B.) RSA.
C.) Diffie-Hellman.
D.) All of the above.

(15) [2 pts.] Which of the following protocols simultaneously uses more than one TCP connection between a client and a server?

A.) SSH.
B.) Finger.
C.) X Windows.
D.) $\boxed{\text{FTP.}}$

(16) [2 pts.] Which protocol is used in the Little Internet to determine the Ethernet address that is associated with a given IP address?

A.) $\boxed{\text{ARP.}}$
B.) RARP.
C.) EthAddress.
D.) IP.

Continued on page 4

(17) [2 pts.] How many collision domains are in the Little Internet?

A.) 6.
B.) 12.
C.) $\boxed{\text{24.}}$
D.) 36.

(18) [2 pts.] Secure Shell (SSH) is a secure replacement for

A.) Telnet.
B.) Rlogin.
C.) FTP.
D.) $\boxed{\text{All of the above.}}$

(19) [2 pts.] Which layer of the TCP/IP Internet Layering Model uses routing tables?

A.) Network Interface Layer.
B.) $\boxed{\text{Internet Layer.}}$
C.) Transport Layer.
D.) Application Layer.

(20) [2 pts.] Which equation best describes the UDP protocol?

A.) UDP = IP.
B.) $\boxed{\text{UDP = TCP - reliability.}}$
C.) UDP = ICMP + protocol ports.
D.) UDP = TCP - IP.

(21) [2 pts.] Which of the following routing protocols uses link-state routing?

A.) GGP.
B.) BGP.
C.) HELLO.
D.) $\boxed{\text{OSPF.}}$

Continued on page 5

(22) [2 pts.] Which network technology provides the highest level of privacy?

A.) Wireless Ethernet.
B.) Ethernet.
C.) FDDI.
D.) $\boxed{\text{ATM.}}$

(23) [2 pts.] Which of the following protocols has the weakest authentication mechanism?

A.) Telnet.
B.) FTP.
C.) $\boxed{\text{TFTP.}}$
D.) Rlogin.

(24) [2 pts.] Which of the following protocols provides reliability?

A.) TCP.
B.) TFTP.
C.) BGP.
D.) $\boxed{\text{All of the above.}}$

(25) [2 pts.] The `traceroute` program normally uses the protocol(s)

A.) UDP.
B.) $\boxed{\text{UDP and ICMP.}}$
C.) TCP and ICMP.
D.) IGMP.

(26) [5 pts.] Fill in the blank. A software specification is to a software implementation as a security <u>policy</u> is to a security posture.

(27) [5 pts.] Answer the following question using no more than two sentences: What assumption about natural number arithmetic is the RSA public key encryption algorithm based on?

Answer: Factoring the product of two large prime numbers is mathematically infeasible without knowing at least one of the prime numbers.

(28) [5 pts.] How many addresses are in a subnet whose mask is 255.255.248.0?

Answer: $2^{3+8} = 2^{11}$.

Continued on page 6

(29) [5 pts.] Answer the following question using no more than two sentences: What is one of the main security concerns of the Domain Name System?

Answer: (1) The Domain Name System (DNS) can be used by an attacker to probe a network. (2) By altering DNS information, an attacker can thwart authentication based on domain names.

(30) [5 pts.] Answer the following question using no more than two sentences: What is the principle of least privilege?

Answer: The principle of least privilege is the idea that a subject should be given the mimimum privileges needed to perform its prescribed task.

(31) [5 pts.] Answer the following question using no more than two sentences: What information is contained in the *acknowledgment number* field of a TCP segment header?

Answer: The acknowledgement number of a TCP segment sent by B to A contains the first octet in the octet stream being transmitted from A to B that B has not yet received.

(32) [5 pts.] Suppose the ownership and access rights of the Unix program `passwd` for changing an account's password are set as follows:

```
Access rights  Owner  Group
-rws---rwx     root   root
```

Using no more than two sentences, explain how an attacker could use this program to take over the host.

Answer: The ownership and access rights of this file say that it runs under root when executed and can be written and executed by any user. Therefore, any user can rewrite the file so that it contains a program that changes the root password to whatever the user desires—which, upon execution, gives the user effective control of the host!

Continued on page 7

(33) [5 pts.] Complete the following table for the first three segments and the last four segments of a TCP connection. (1 means the flag is set, 0 means it is not.)

Segment	ACK	SYN	FIN
1	0	1	0
2	1	1	0
3	1	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-3$	1	0	1
$n-2$	1	0	0
$n-1$	1	0	1
n	1	0	0

(34) [10 pts.] Recall the diagram of a conventional internet using the TCP/IP protocols (which is not shown).

$\mathsf{I}_1, \ldots, \mathsf{I}_7$ are interfaces to the single physical networks $\mathsf{SPN}_1, \ldots, \mathsf{SPN}_5$. $\mathsf{J}_1, \mathsf{J}_2, \mathsf{J}_3$ are interfaces to loopback networks. $\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3$ are hosts. There are other hosts and interfaces that are not shown. The following table shows what IP addresses and subnet masks are assigned to the $\mathsf{I}_1, \ldots, \mathsf{I}_7$ interfaces.

Interface	**IP Address**	**Subnet Mask**
I_1	201.99.01.5	255.255.255.0
I_2	201.99.02.66	255.255.255.240
I_3	201.99.02.67	255.255.255.240
I_4	156.102.87.53	255.255.0.0
I_5	201.99.03.76	255.255.255.0
I_6	201.99.03.75	255.255.255.0
I_7	201.99.04.98	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 in S for the "next hop" ($r = *$ for direct routes).
- i is an interface.

Continued on page 8

Write down the routing table for H_2 as a list of (a, m, r, i) tuples. Do not use any host-specific routes.

Answer:

$$
\begin{array}{lrrrll}
(& 127.0.0.0, & 255.0.0.0, & *, & \mathsf{J}_2 &) \\
(& 201.99.02.64, & 255.255.255.240, & *, & \mathsf{I}_3 &) \\
(& 156.102.0.0, & 255.255.0.0, & *, & \mathsf{I}_4 &) \\
(& 201.99.03.0, & 255.255.255.0, & *, & \mathsf{I}_5 &) \\
(& 201.99.01.0, & 255.255.255.0, & 201.99.02.66, & \mathsf{I}_3 &) \\
(& 201.99.04.0, & 255.255.255.0, & 201.99.03.75, & \mathsf{I}_5 &)
\end{array}
$$