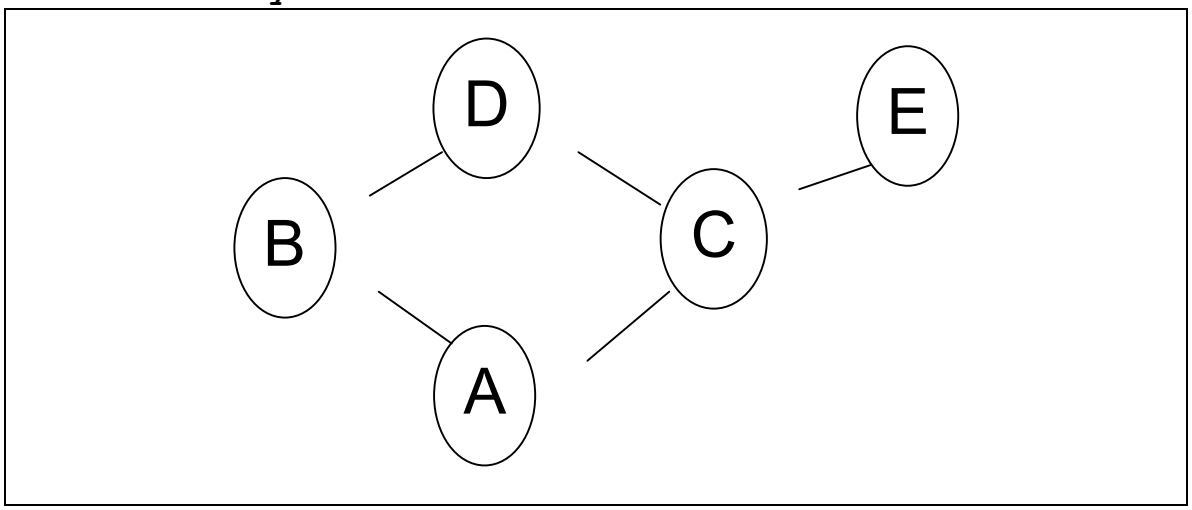
# Sample Solution and Comments for Quiz #3

1. **(8 points)** Translate the following RBAC system configuration into a DAC system. The RBAC system consists of the following role hierarchy, permission assignment table, and user assignment table:

**Role hierarchy:**




**Permission assignment**

| | | Permissions (Object, operation) | | | | |
|---|---|---|---|---|---|---|
| | | $(O_1,M_1)$ | $(O_1,M_2)$ | $(O_2,M_1)$ | $(O_2,M_2)$ | $(O_3,M_1)$ |
| Roles | A | √ | | | | |
| | B | | √ | | | √ |
| | C | | | √ | | |
| | D | | | | √ | |
| | E | | | | | √ |

**User assignment**

| | | Users | | | | |
|---|---|---|---|---|---|---|
| | | $U_1$ | $U_2$ | $U_3$ | $U_4$ | $U_5$ |
| Roles | A | √ | | | | |
| | B | | √ | | | |
| | C | | | √ | | |
| | D | | | | √ | |
| | E | | | | | √ |

To answer this question, fill out the following access matrix (follow the example for $U_1$):

| | | Objects | | |
|---|---|---|---|---|
| | | $O_1$ | $O_2$ | $O_3$ |
| Subjects | $U_1$ | $M_1$ | | |
| | $U_2$ | M1,M2 | | M1 |
| | $U_3$ | M1 | M1 | |
| | $U_4$ | M1,M2 | M1,M2 | M1 |
| | $U_5$ | M1 | M1 | M1 |

2. **(5 points)** Suppose a remote host begins the TCP three-way hand-shake with the local host but never send final ACK packet. This is called a ***half-open connection***. The local host waits for some short time and then purges the information from its network tables. If a remote host makes so many half-open connections that the local host cannot accept connections from other hosts, the remote host has launched a ***syn flood attack***.

   Write logging (i.e., what should be written into the log) and auditing requirements (i.e., on which condition should an analyzer trigger alarm) to detect such an attack. Explain your answer.

The log should contain an entry for each three way handshake initiated which includes the remote IP. This entry should be flagged if the connection was terminated as half open.

An alarm should be triggered if either:

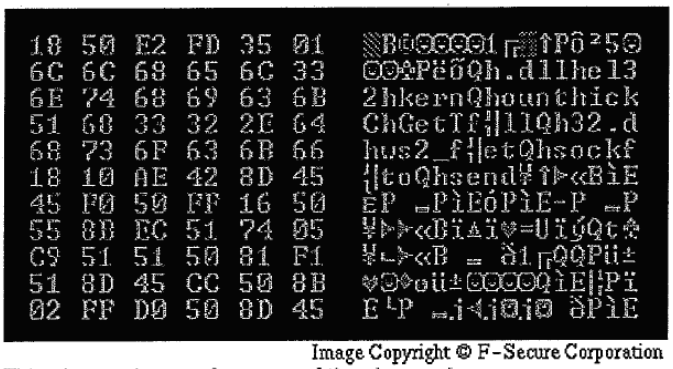
- A single remote host initiates more than x half-open connections in a given time
- The number of half-open connections from all remote hosts exceeds y% of the local machine's capacity.

x and y would be chosen based on the local machine.

*Contributed by Neale Genereux*

3. **(6 points)** The following is a fragment of Slammer worm description from F-Secure Corporation. Use the space after the description to explain how the worm does the following standard functions: Reconnaissance, Attack, Communication, Command, Intelligence. If necessary, make reasonable assumptions and state them clearly.
Sample answer:

addresses multiplies the network load generated by the worm.



```
18 50 E2 FD 35 01   ▒P▒▒▒▒1┌▒↑Pô²5☺
6C 6C 68 65 6C 33   ☺☺♣PëõQh.dllhel3
6E 74 68 69 63 6B   2hkernQhounthick
51 68 33 32 2E 64   ChGetTf╢llQh32.d
68 73 6F 63 6B 66   hus2_f╢etQhsockf
18 10 AE 42 8D 45   ╢toQhsend╫↑►«BìE
45 F0 50 FF 16 50   EP ▬PìEóPìE-P ▬P
55 8D EC 51 74 05   ¥►►«DïAï♥=UiýQt♣
C9 51 51 50 81 F1   ¥└►«B ▬ ð1┌QQPü±
51 8D 45 CC 50 8B   ♥☺♦oü±☺☺☺☺QìE╢Pï
02 FF D0 50 8D 45   E╙P ▬.i◄.i◘.i◘ ðPìE
```

Image Copyright © F-Secure Corporation

This picture shows a fragment of the virus code

Since the worm code does not have any delay in the scanning loop it generates massive amount of network traffic as a side effect.

Slammer does not have any intentional payload or strings inside.

Recon: Infinite loop that scans for random vulnerable hosts on internet. ✓

Attak: Sends itself to computers on UDP 1434 to cause buff. overflow for MSSQL 2000 servers.

Commun.: No communication between worms. All scanning is done randomly. Assumes worm will re-infect an infected server. ✓

Command: No command option. Worm is autonomous and uncontrolled.

Intel: None since assumed that worm doesn't keep track of other infected servers and just generates traffic by itself, randomly.

*Contributed by Shane Wang*

**Comments:**

1. **Most people did well on question 1.**
2. **Some people were logging too much information for question 2. The standard answer is, logger should write hand-shake time out events when remote machine initiates the handshake; analyzer should trigger an alarm when the frequency of time-outs exceeds a specified threshold.**
3. **Nobody has answered question 3 100% correct. The answer is, paragraph 3 is Attack, paragraph 5 is Reconnaissance, and paragraph 6 is Attack. There is no Communication, Command, or Intelligence.**