

## 1D0-470 Security Professional

Which of the following choices lists the ports that Microsoft internal networking uses that should be blocked from outside access?

- A. UDP 137 and 138, and TCP 139
- B. Ports 11, 112, and 79
- C. UDP 1028, 31337 and 6000
- D. Port 80, 134 and 31337

**Answer:** D

What is the best way to keep employees on a LAN from unauthorized activity or other mischief?

- A. Reduce each user's permissions to the minimum needed to perform the tasks required by his or her job.
- B. Limit the number of logins available to all users to one at a time.
- C. Limit the number of files that any one user can have open at any given time.
- D. Implement a zero-tolerance policy in regard to employees who load games or other unauthorized software on the company's computers.

**Answer:** A

What is a spoofing attack?

- A. A hacker pretends to be the superuser and spoofs a user into allowing him into the system.
- B. A hacker calls a user and pretends to be a system administrator in order to get the user's password.
- C. A computer (or network) pretends to be a trusted host (or network).
- D. A hacker gains entrance to the building where the network resides and accesses the system by pretending to be an employee.

**Answer:** C

Abjee is going to log on to his network. His network does not employ traffic padding mechanisms. Why will it be easy for someone to steal his password?

- A. Because his password could be more than two weeks old
- B. Because of the predictability of the length of the login and password prompts
- C. Because the clear text user name and password are not encrypted
- D. Because there is no provision for log analysis without traffic padding, thus no accountability when passwords are lost

**Answer:** B

**#End Demo#**