# Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/16/2022 9:47:45 pm • Time spent: 03:19

Score: 70% Passing Score: 80%

**Question 1:** ✕ Incorrect

You have placed a File Transfer Protocol (FTP) server in your DMZ behind your firewall. The FTP server is to be used to distribute software updates and demonstration versions of your products. However, users report that they are unable to access the FTP server.

What should you do to enable access?

- Install a VPN.
- Define user accounts for all external visitors.
- Open ports 20 and 21 for inbound and outbound connections.
- ~~Move the FTP outside of the firewall.~~

EXPLANATION

To allow FTP traffic into your DMZ, you must open the correct ports on the firewall. For FTP, the correct ports are 20 and 21 for outbound connections.

Installing a VPN is not necessary to grant access to external users. Defining user accounts may be required in some situations, but this scenario requires anonymous access. Moving the FTP server outside the firewall is not a secure action.

**Question 2:** ✔ Correct

FTPS uses which mechanism to provide security for authentication and data transfer?

- Multi-factor authentication
- Token devices
- ➡ SSL
- IPsec

EXPLANATION

File Transfer Protocol Secure (FTPS) uses Secure Sockets Layer (SSL) to provide security for authentication and data transfer. FTPS is an FTP replacement that brings reasonable security to an otherwise unsecure file-transfer mechanism. FTP by itself is unsecure because FTP transmits logon credentials in cleartext and does not encrypt transmitted files.

**Question 3:** ✔ Correct

To transfer files to your company's internal network from home, you use FTP. The administrator has recently implemented a firewall at the network perimeter and disabled as many ports as possible.

Now, you can no longer make the FTP connection. You suspect the firewall is causing the issue. Which ports need to remain open so you can still transfer the files? (Select two.)

- 443
- ➡ 20
- 80
- 23
- ➡ 21

EXPLANATION

FTP uses port 21 for connection requests and port 20 for data transfers. Both ports need to remain open for you to transfer files to your company's internal network from home.

Telnet uses port 23, SSL uses port 443, and HTTP uses port 80.

**Question 4:** ✕ Incorrect

You want to close all ports associated with NetBIOS on your network's firewalls to prevent attacks directed against NetBIOS. Which ports should you close?

- 67, 68
- 135, 137-139
- ~~161, 162~~
- 389, 636

EXPLANATION

NetBIOS uses the following ports:

- TCP 135
- TCP and UDP 137
- TCP and UDP 138
- TCP 139

Dynamic Host Configuration Protocol (DHCP) uses ports 67 and 68. Simple Network Management Protocol (SNMP) uses ports 161 and 162. Lightweight Directory Access Protocol (LDAP) uses ports 389 and 636.

**Question 5:** ✕ Incorrect

Which of the following file transfer protocols use SSH to provide confidentiality during the transfer? (Select two.)

- [ ] FTPS
- [ ] FTP
- [x] ~~HTTPS~~
- [x] SFTP
- [ ] SCP

EXPLANATION

Secure Copy Protocol (SCP) and SSH File Transfer Protocol (SFTP) both use SSH to provide confidentiality.

FTPS and HTTPS both use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to provide confidentiality.

File Transfer Protocol (FTP) is an older TCP/IP protocol that's used for transferring files across systems.

**Question 6:** ✓ Correct

To increase security on your company's internal network, the administrator has disabled as many ports as possible. However, now you can browse the internet, but you are unable to perform secure credit card transactions.

Which port needs to be enabled to allow secure transactions?

- (•) 443
- ( ) 69
- ( ) 23
- ( ) 80
- ( ) 21

EXPLANATION

To perform secure transactions, SSL on port 443 needs to be enabled. HTTPS uses port 443 by default.

**Question 7:** ✔ Correct

You have a shared folder named Reports. Members of the Managers group have been given Write access to the shared folder.

Mark Mangum is a member of the Managers group. He needs access to the files in the Reports folder, but he should not have any access to the Confidential.xls file.

What should you do?

- Add Mark Mangum to the ACL for the Reports directory with Deny permissions.
- Configure NTFS permissions for Confidential.xls to allow read-only.
- Remove Mark Mangum from the Managers group.
- ➡ Add Mark Mangum to the ACL for the Confidential.xls file with Deny permissions.

EXPLANATION

To prevent Mark from accessing one file, edit the ACL for that file, add his user account to the ACL, and configure Deny permissions. The Deny permissions configured on the file override the Write permissions granted to the folder through the group.

Removing Mark from the group would prevent access to the entire folder, not just to the one file. Configuring Deny permissions to the folder for Mark would also prevent access to the entire folder.

**Question 8:** ✔ Correct

You want to give all managers the ability to view and edit a certain file. To do so, you need to edit the discretionary access control list (DACL) associated with the file. You want to be able to easily add and remove managers as their job positions change.

What is the BEST way to accomplish this?

- ➡ Create a security group for the managers. Add all users as members of the group. Add the group to the file's DACL.
- Add one manager to the DACL that grants all permissions. Have this user add other managers as required.
- Create a distribution group for the managers. Add all users as members of the group. Add the group to the file's DACL.
- Add each user account to the file's DACL.

EXPLANATION

Create a security group for the users and add the users to the DACL. A group is an object that identifies a set of users with similar access needs. Microsoft systems have two kinds of groups, which are distribution groups and security groups. Only security groups can be used for controlling access to objects. As manager roles change, add or remove user accounts from the group. Assigning permissions to a group grants those same permissions to all members of the group.

Adding individual user accounts instead of groups to the ACL would require more work as you add or remove managers.

**Question 9:** ✔ Correct

If Mark has a read-write permission to the share \\fileserver\securefiles and a read-only permission to the file coolstuff.docx on the NTFS file system shared by the file share, he is able to perform which action?

- ➡ Read the file.
- Change the contents of the file.
- Rename the file.
- Delete the file.

EXPLANATION

The permissions of the share and file system work together, and the more restrictive of the two is used when accessing the file through the share. In this case, Mark is allowed to read the file.

Because the NTFS permissions are set to read-only, he would not be allowed to delete, rename, or change the file.

**Question 10:** ✔ Correct

You have a file server named Srv3 that holds files used by the development department. You want to allow users to access the files over the network and control access to files accessed through the network or through a local logon.

Which solution should you implement?

- Share permissions and quotas
- NTFS permissions and file screens
- ➡ NTFS and share permissions
- Share permissions and file screens

EXPLANATION

Use New Technology File System (NTFS) and share permissions to control access to files. Share permissions apply when files are accessed through the network, and NTFS permissions apply to both network and local access.

Use file screens to restrict the types of files that can be saved within a folder.