Exam Report: 7.5.7 Practice Questions

Date: 1/22/2020 5:51:16 pm
Time Spent: 6:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 62%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You want to close all ports associated with NetBIOS on your network 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

DHCP uses ports 67 and 68. SNMP uses ports 161 and 162. LDAP uses ports 389 and 636.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_01]

Question 2: Correct

Which of the following ports does FTP use to establish sessions and manage traffic?

- 135 - 139
- 25, 110
- 80, 443
- 20, 21

Explanation

FTP uses ports 20 and 21 to establish sessions and manage traffic. Once sessions are established, FTP uses a random higher order port (above 1024) to perform the actual file transfers.

Port 80 is used by HTTP and TLS. Port 443 is used by SSL and TLS. Port 25 is used by SMTP, and port 110 is used by POP3. Ports 135 - 139 are used by NetBIOS.

References

LabSim for Security Pro, Section 7.5.

[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_02]

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.)

- [ ] 23
- [x] 21
- [ ] 443
- [ ] 80
- [x] 20

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.

References

LabSim for Security Pro, Section 7.5.

[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_03]

Question 4: Correct

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

Which port needs to be enabled to allow secure transactions?

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

Explanation

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

References

LabSim for Security Pro, Section 7.5.

[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_04]

Question 5: Incorrect

Which of the following network services or protocols uses TCP/IP port 22?

- ( ) SSH
- ( ) NNTP
- (•) ~~TFTP~~
- ( ) IMAP4

Explanation

The Secure Shell service (SSH) uses TCP/IP port 22. SSH is a terminal emulation program similar to Telnet, which provides secure authenticated sessions on a remote system. It is most commonly associated with Unix and Linux systems.

The Trivial File Transfer Protocol (TFTP) is a connectionless service for downloading files from a remote system. TFTP uses TCP/IP port 69. The Network News Transfer Protocol (NNTP) is used to access and download messages from newsgroup servers. NNTP uses TCP/IP port 119. The Internet Message Access Protocol version 4 (IMAP4) is used to download emails from remote servers. IMAP 4 uses TCP/IP port 143.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_05]

Question 6: Correct

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

- (selected) SSL
- Token devices
- IPsec
- Multi-factor authentication

Explanation

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

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_06]

Question 7: 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?

- Add one manager to the DACL that grants all permissions. Have this user add other managers as required.
- (selected) Create a security group for the managers. Add all users as members of the group. Add the group to the file's DACL.
- 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, *distribution* and *security*. 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.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_07]

Question 8: Incorrect

You have two folders that contain documents used by various departments:

- The Development group has been given the Write permission to the Design folder.
- The Sales group has been given the Write permission to the Products folder.

No other permissions have been given to either group.

User Mark Tillman needs to have the Read permission to the Design folder and the Write permission to the Products folder. You want to use groups as much as possible.

What should you do?

- ~~Make Mark a member of the Development group; add Mark's user account directly to the ACL for the Products folder.~~
- Make Mark a member of the Development and Sales groups.
- Make Mark a member of the Sales group; add Mark's user account directly to the ACL for the Design folder.
- Add Mark's user account directly to the ACL for both the Design and Products folders.

Explanation

Make Mark a member of the Sales group to give him the Write permission to the Products folder. Add Mark's user account to the ACL for the Design folder and grant the Read permission.

Adding Mark as a member of the Development group would give him too much permission to the Design folder. Adding Mark to the ACL for both folders would not use groups when possible.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_08]

Question 9: Incorrect

You have multiple users who are computer administrators. You want each administrator to be able to shut down systems and install drivers.

What should you do? (Select two.)

- [ ] Create a distribution group for the administrators and add all user accounts to the group.
- [x] Grant the group the necessary user rights.
- [ ] Create a security group for the administrators and add all user accounts to the group.
- [ ] Add the group to the DACL.
- [ ] Add the group to the SACL.

Explanation

Create a security group for the users and grant the group the necessary user rights. On a Microsoft system, a *user right* is a privilege or action that can be taken on the system, such as logging on, shutting down the system, backing up the system, or modifying the system date and time. Permissions apply to objects (files, folders, printers, etc.), while user rights apply to the entire system (computer).

A *group* is an object that identifies a set of users with similar access needs. Microsoft systems have two kinds of groups:, *distribution* and *security*. Only security groups can be used to control access to objects. As manager roles change, add or remove user accounts from the group.

A system access list (SACL) is used by Microsoft for auditing to identify past actions performed by users

on an object. A discretionary access list (DACL) is an implementation of discretionary access control (DAC). Owners add users or groups to the DACL for an object and identify the permissions allowed for that object.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_09]

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 a local logon.

Which solution should you implement?

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

Explanation

Use 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.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_10]

Question 11: Incorrect

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 should not have any access to the Confidential.xls file.

What should you do?

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

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 permission 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.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_11]

Question 12: Correct

You have placed an FTP server in your DMZ behind your firewall. The FTP server will be used to distribute software updates and demonstration versions of your products. Users report that they are unable

to access the FTP server.
What should you do to enable access?

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

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 using accounts may be required in some situations, but this one requires anonymous access. Moving the FTP server outside the firewall is not a secure action.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_12]

Question 13: Incorrect

Many popular operating systems allow quick and easy file and printer sharing with other network members. Which of the following is **not** a means by which file and printer sharing is hardened?

- Hosting all shared resources on a single centralized and secured server
- (selected) ~~Imposing granular access control via ACLs~~
- Allowing NetBIOS traffic outside of your secured network
- Logging all activity

Explanation

Hardening file and printer sharing does not include allowing NetBIOS traffic to pass out of or into a secured network. NetBIOS is notoriously insecure and should not be permitted to exit or enter any secured network.

Hardening file and printer sharing does include ACLs, logging, and centralized resource servers.

References

LabSim for Security Pro, Section 7.5.
[All Questions SecPro2017_v6.exm FILE_SERVER_SEC_13]