02: Lab 02 - Assisted - Configuring examples of security control types

Security+ (Exam SY0-701)

Congratulations, you passed!

Duration: 50 minutes, 14 seconds

☑ Which account or group object on the access control list should NOT have been assigned permissions on the share? *Score: 1*

- ● Users
- ○ Domain Admins
- ○ LocalAdmin
- ○ CREATOR OWNER

Congratulations, you have answered the question correctly.

☑ **check if the Users group has access to '\\10.1.16.1\TOOLS' share** *Score: 1*

Select the **Score** button to validate this task:

```
No access for 'Domain Users' to SMB Share 'TOOLS'

Task complete
```

☑ File access controls are classed as preventive in terms of functionality. What category of security control are file permissions? *Score: 1*

- ● Technical
- ○ Managerial
- ○ Operational
- ○ Physical

Congratulations, you have answered the question correctly.

☑ **confirm if the C:\LABFILES\empty directory was deleted** *Score: 1*

Select the **Score** button to validate this task:

```
C:\LABFILES\empty deleted ...

Task complete
```

☑ The results of the find operation indicate what? *Score: 1*

- ○ Jamie is an administrator
- ● Folder deletion is not being audited
- ○ Users are unable to access empty folders

○ User activity is being tracked

Congratulations, you have answered the question correctly.

☑ **confirm if the C:\LABFILES\pcaps directory was deleted and check for an event log record with an event ID of 4663 and an Object Name of C:\LABFILES\** *Score: 1*

Select the **Score** button to validate this task:

```
C:\LABFILES\pcaps deleted ...

Event log record found with ID 4663 and Object Name C:\LABFILES\pcaps

Task complete
```

☑ What is the purpose of a detective control? *Score: 1*

○ Deny access to an object
○ Notify subjects about system policies
○ Inform users of the proper steps to perform an activity
● Create a record of events and activities

Congratulations, you have answered the question correctly.

☑ **confirm the existence of LegalNoticeCaption and LegalNoticeText registry keys with non-zero values $result = $False** *Score: 1*

Select the **Score** button to validate this task:

```
Registry keys LegalNoticeCaption and LegalNoticeText exist

Task complete
```

☑ What is the goal of directive controls? *Score: 1*

○ Defense
● Compliance
○ Prohibition
○ Tracking

Congratulations, you have answered the question correctly.

☑ What are the dual purposes of corrective controls? (Select two) *Score: 1*

☑ Address an unwanted or less secure state or event
☐ Record evidence of user and event activities
☑ Return the system to a normal and generally secure condition
☐ Provide guidance on proper user behavior

Congratulations, you have answered the question correctly.

☑ **confirm if the notes.txt file exists and contains "This is important"** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\notes.txt exists and contains 'This is important'

Task complete
```

☑ **confirm if C:\Users\jaime\hash.txt exists and is not empty** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\hash.txt exists

Task complete
```

☑ **confirm if the calchash.ps1 file exists and contains the "Get-FileHash" command** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\calchash.ps1 exists and contains the 'Get-FileHash' command

Task complete
```

☑ **confirm if the check.ps1 file exists and contains the "Get-Content" cmdlet** *Score: 1*

Select the **Score** button to validate this task:

```
File C:\Users\jaime\check.ps1 exists and contains the 'Get-Content' cmdlet

Task complete
```

☑ What is the typical means (which was used in this exercise) to detect changes in a file? *Score: 1*

- ○ encryption
- ○ authentication
- ○ authorization
- ● hashing

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of preventive controls? *Score: 1*

- ● Stop unwanted activity from succeeding
- ○ Record information about activities
- ○ Give instructions
- ○ Restore a system back to preferred condition
- ○ Persuade a perpetrator to go elsewhere
- ○ Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of detective controls? *Score: 1*

- ○ Stop unwanted activity from succeeding
- ● Record information about activities
- ○ Give instructions
- ○ Restore a system back to preferred condition
- ○ Persuade a perpetrator to go elsewhere
- ○ Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of directive controls? *Score: 1*

- ○ Stop unwanted activity from succeeding

○ Record information about activities
● Give instructions
○ Restore a system back to preferred condition
○ Persuade a perpetrator to go elsewhere
○ Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the primary purpose of corrective controls? *Score: 1*

○ Stop unwanted activity from succeeding
○ Record information about activities
○ Give instructions
● Restore a system back to preferred condition
○ Persuade a perpetrator to go elsewhere
○ Compensate for a failed control

Congratulations, you have answered the question correctly.

☑ What is the purpose of the dot and slash in front of the filenames in the PowerShell scripts and when executing PowerShell scripts? *Score: 1*

○ Allow for administrator execution
● Reference the current working directory
○ To set the security content of the process
○ For avoiding detection by an IDS

Congratulations, you have answered the question correctly.