CompTIA A+ Core 2 Exam 220-1102

Lesson 19

Using Support and Scripting Tools

Objectives

- Use remote access technologies
- Implement backup and recovery
- Explain data handling best practices
- Identify basics of scripting

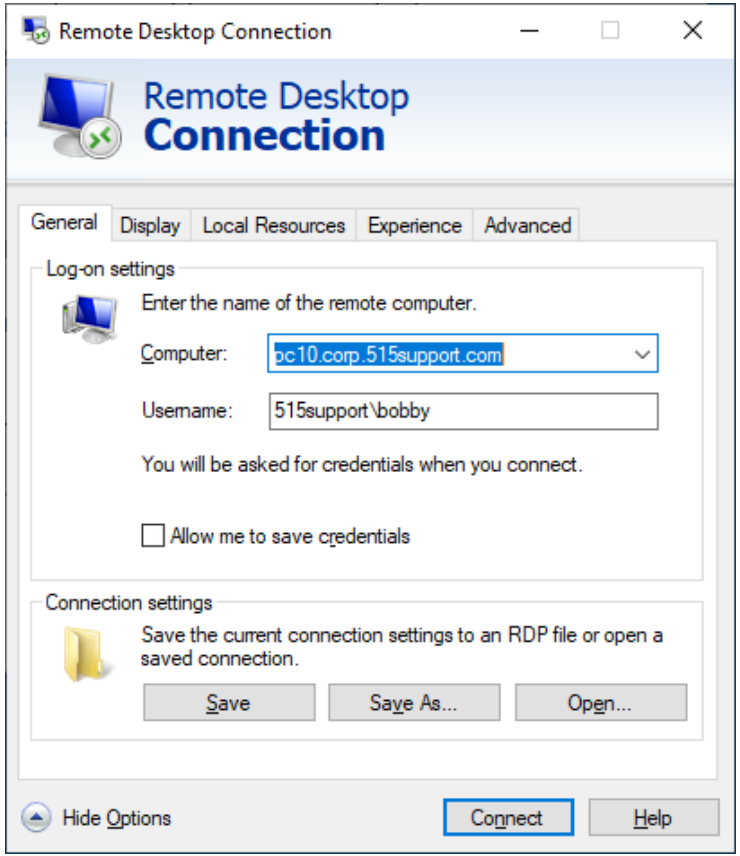
Lesson 19

Topic 19A

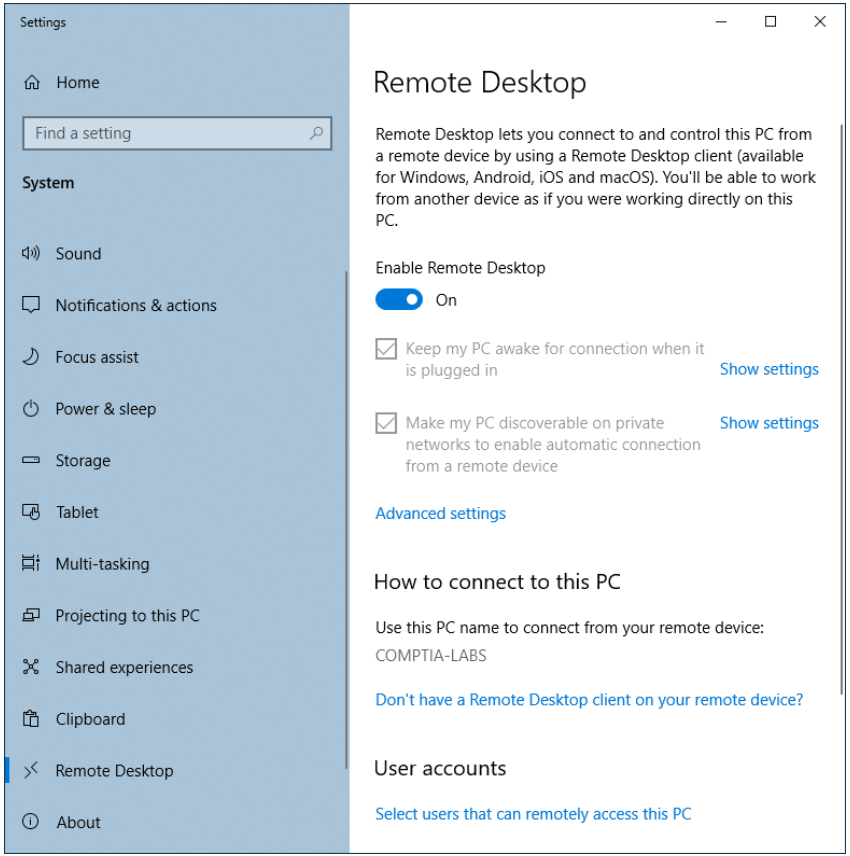
Use Remote Access Technologies

Remote Desktop Tools

- Security considerations
  - Granting access
  - Preventing snooping
  - Patching vulnerabilities
- Remote Desktop Protocol (RDP)
  - mstsc.exe client app and session encryption
  - Multi-platform RDP clients
- Virtual Network Computing (VNC)
  - macOS Screen Sharing
  - Secure versus unsecure third-party implementations



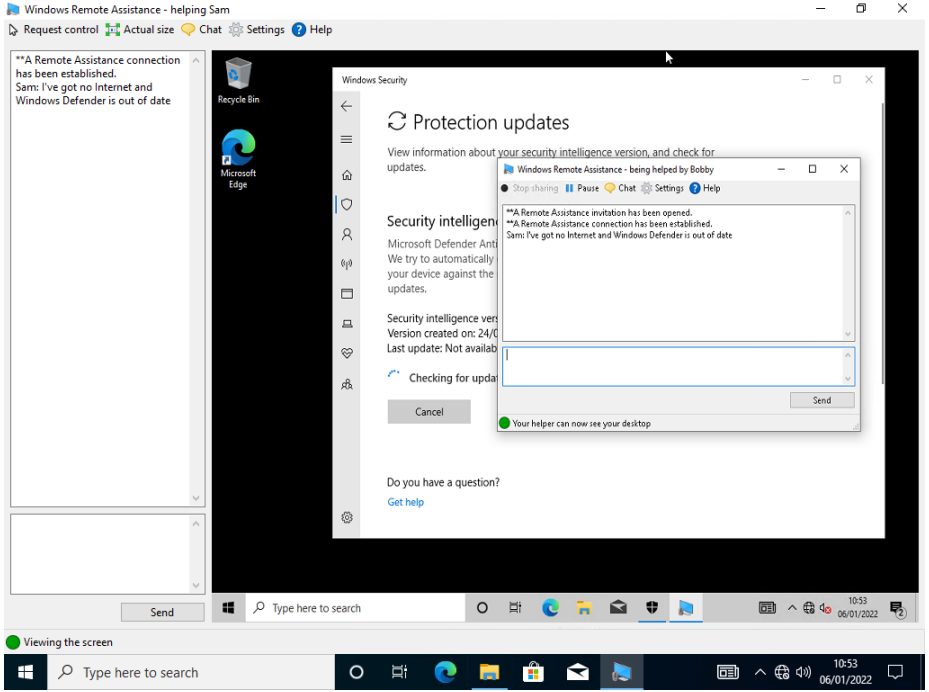
RDP Server and Security Settings



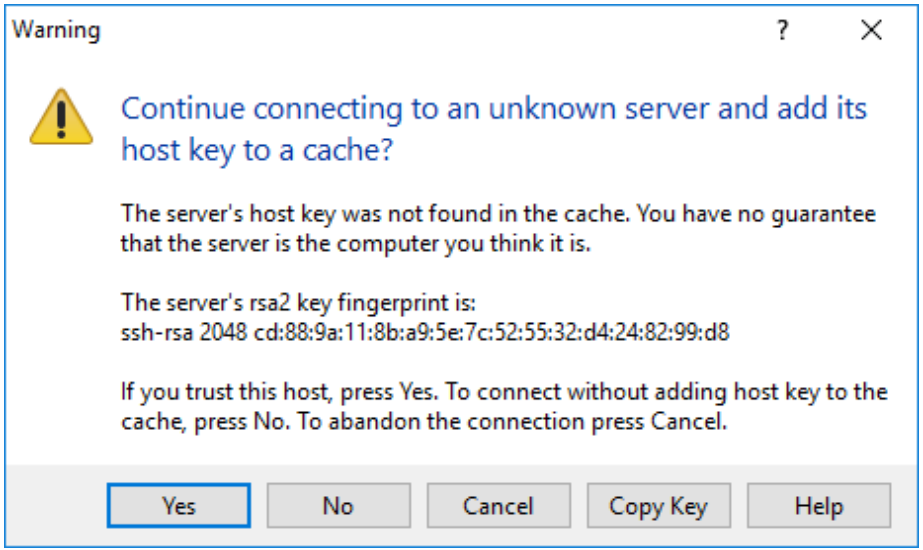
- Security considerations
  - Accounts allowed to connect
  - Network Level Authentication (NLA)
  - RDP Restricted Admin (RDPRA) Mode and Remote Credential Guard
  - TCP/3389 and risks from allowing port forwarding
- Open-source RDP servers

Microsoft Remote Assistance

- Allows users to send invite to connect over RDP protected by password
- Chat and request control features
- Quick Assist feature better suited to connections over the Internet



Secure Shell



- Remote terminal access to command-line shell
- Secure Shell (SSH) server
  - Server's host key
  - TCP/22
- SSH client
  - Password authentication
  - Public key authentication

Desktop Management and Remote Monitoring Tools

- Visibility
  - Remote monitoring and management (RMM)
  - Desktop management and unified endpoint management (UEM)
- Common features
  - Performance monitoring and log collection
  - Security scanning
  - Push deployment
  - Remote support
- Intel vPRO/AMD PRO hardware support for out-of-band (OOB) remote access

Other Remote Access Tools

- Screen-sharing software
  - Third-party remote desktop tools designed to work over the Internet
- Video-conferencing software
  - Most include a basic screen share client
- File transfer software
  - Easy sharing via Bluetooth
  - Apple AirDrop, Windows Nearby Sharing, and Android Nearby Share
- Virtual private network (VPN)
  - Connect the remote host to the local network over a secure tunnel
  - Can be more secure than opening or port forwarding remote desktop/SSH ports

Review Activity: Remote Access Technologies

- Remote Desktop Tools
- RDP Server and Security Settings
- Microsoft Remote Assistance
- Secure Shell
- Desktop Management and Remote Monitoring Tools
- Other Remote Access Tools

Lab Activity

- Assisted Lab: Use Remote Access Technologies
  - Use RDP and SSH to connect to Windows and Linux hosts over a network

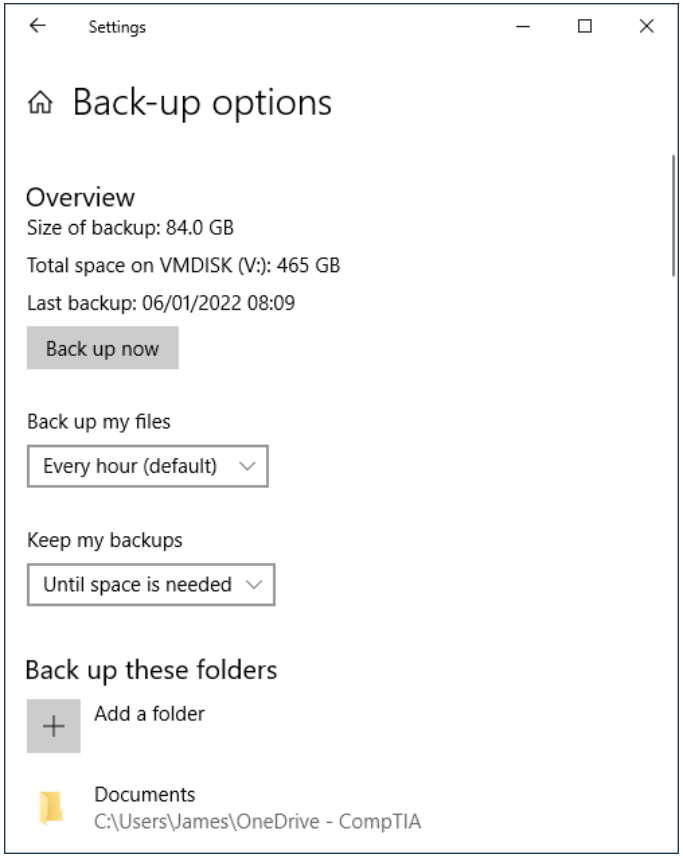
Lesson 19

Topic 19B

Implement Backup and Recovery

Backup Operations

- Criticality of data backup and recovery operations
  - What to back up
  - How to store backups
  - Testing and validating recovery procedures
- Windows tools for personal data backups
  - File History
  - Windows Backup and Restore Center



Backup Methods

- Frequency and retention
- Backup chains
  - Full with incremental or differential
- Synthetic backup
  - Reduces transfer requirements by synthesizing next full backup from incremental jobs

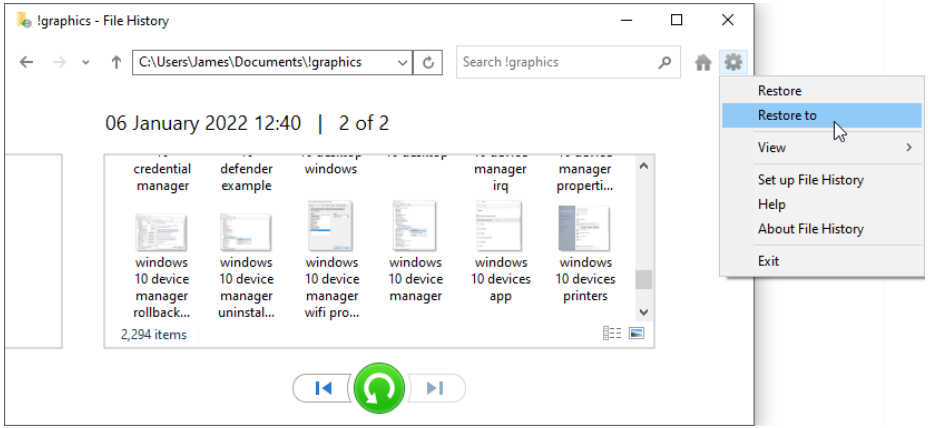
Type	Data Selection	Backup Job Time and Storage Requirement	Recovery Complexity	Archive Attribute
Full	All selected data regardless of when it was previously backed up	High	Low (single job)	Cleared
Incremental	New files and files modified since last backup job	Low	High (multiple jobs)	Cleared
Differential	New files and files modified since last full backup job	Moderate	Moderate (two jobs)	Not Cleared

Backup Media Requirements

- Grandfather-father-son (GFS) media rotation
  - Label tapes for monthly, weekly, and daily backup jobs
- On site versus off site
- Online versus offline
- 3-2-1 backup rule

Backup Testing and Recovery Best Practices

- Test restore
  - Alternate location
- Verification
  - Data validation via hashing
  - Media integrity
- Check configuration
  - Are all necessary locations/files included?
- Frequent testing



Review Activity: Backup and Recovery

- Backup Operations
- Backup Methods
- Backup Media Requirements
- Backup Testing and Recovery Best Practices

Lab Activity

- Assisted Lab: Implement Backup and Recovery
  - Configure Windows backup and use it to restore files

Lesson 19

Topic 19C

Explain Data Handling Best Practices

Regulated Data Classification

- Regulated data types
  - Personally identifiable information (PII)
  - Personal government-issued information
  - Healthcare data
  - Credit card transactions
- Data handling best practices
- Data retention requirements

Prohibited Content and Licensing Issues

- Prohibited content
- Software licensing
  - End-user license agreement (EULA)
  - License compliance monitoring
    - Valid licenses
    - Expired licenses
  - Open-source licenses
- Digital rights management (DRM)

Incident Response

- Security incident types
- Computer Security Incident Response Team (CSIRT)
  - First responder
  - Inform management/law enforcement

Data Integrity and Preservation

- Nature of digital forensic evidence
- Documentation of incident and recovery of data
  - Identify scope, record scene, and isolate hosts/devices
  - Use live forensic tools or video to extract data from systems that are still powered on
  - Use write blocking imaging tools to make copies of fixed and removable disks
  - Use hashing to validate integrity of images
  - Bag and tag physical drives/devices
- Chain of custody

Data Destruction Methods

- Remnant removal for repurposing and recycling
- Standard formatting (OS format tools)
  - Risk of recoverable data remnants
- Erasing/wiping
  - Hard disks versus solid state disks
- Low level formatting
  - Secure Erase (SE)
  - Instant Secure Erase (ISE)/Crypto Erase

Disposal and Recycling Outsourcing Concepts

- Specialist destruction machinery
  - Shredding, incinerating, degaussing
- Outsourcing concepts
  - Third-party vendor
  - Certification of destruction/recycling
- DIY destruction methods
  - Drilling and hammering

Review Activity: Data Handling Best Practices

- Regulated Data Classification
- Prohibited Content and Licensing Issues
- Incident Response
- Data Integrity and Preservation
- Data Destruction Methods
- Disposal and Recycling Outsourcing Concepts

Lesson 19

Topic 19D

Identify Basics of Scripting

Shell Scripts

- Development environments
  - Shell scripting languages
  - General-purpose scripting languages
  - Programming languages
  - Editors and integrated development environments (IDEs)
- Linux shell scripts (.SH)
  - Shebang
  - Execute permission

```
  1 #!/bin/bash
  2 echo 'Hello World'
~
~
~
:set number                              2,18          All
```

```
toor@LX20D:~$ chmod u+x hello.sh; ls -l $_
-rwxrw-r-- 1 toor toor 31 Jan 11 10:02 hello.sh
toor@LX20D:~$ ./hello.sh
Hello World
toor@LX20D:~$
```

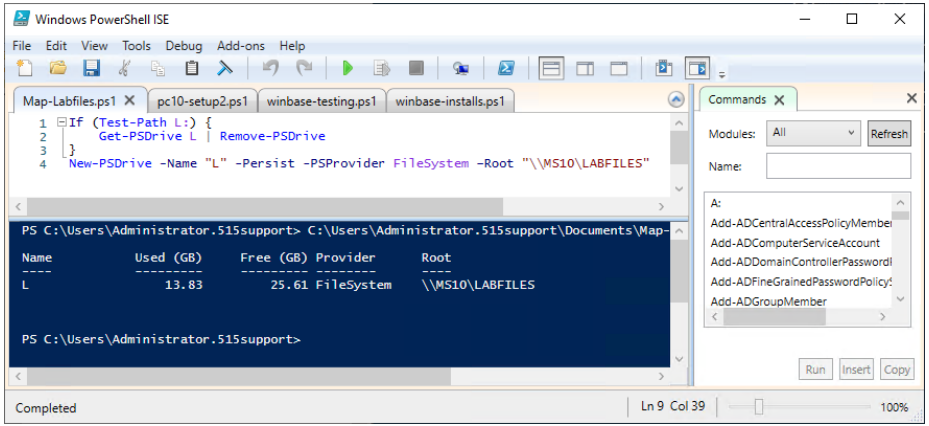
Basic Script Constructs

- Comments
- Identifiers (variables and constants)
- Conditional branch
  - If … Then
- Loops
  - For
  - While
- Operators

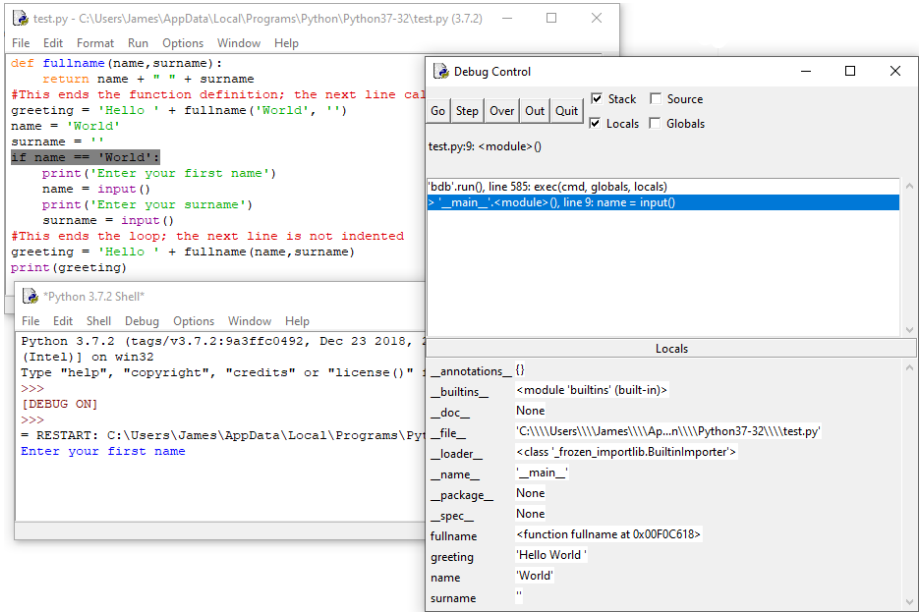
```
#!/bin/bash

# Demonstrate If syntax in Bash

if [ -z “$1” ]

then

    echo ‘Hello World’

else

    echo “Hello $1”

fi
```

Windows Scripts

- PowerShell (.PS1)
  - Cmdlets
  - PowerShell Integrated Scripting Environment (ISE)
- VisualBasic Script (.VBS)
  - Earlier Windows scripting environment
- Batch files (.BAT)
  - Original cmd shell environment



JavaScript and Python



- JavaScript (.JS)
  - Mostly used for web applications and mobile apps
  - macOS JavaScript for Automation (JXA)
- Python (.PY)
  - Scripting and creating executable software
  - Interpreters (CPython, PyPy, …)
  - Python2 versus Python3

Use Cases for Scripting

- Interacting with operating systems
  - Native commands
  - OS application programming interface (API) and scripting libraries/modules
- Use cases for basic automation
  - Restarting machines
  - Remapping network drives
  - Installation of applications
  - Initiating updates
  - Automated backups
  - Gathering of information/data

```
If (Test-Path L:) {
    Get-PSdrive L | Remove-PSDrive
}
New-PSDrive -Name “L” -Persist -PSProvider
FileSystem -Root “\\MS10\LABFILES”
```

Scripting Best Practices and Considerations

- Malware risks
  - Unauthorized modification of source code
  - Increasing attack surface and exposing vulnerabilities
- Inadvertently changing system settings
  - Lock out due to changing firewall configuration
  - Disabling security features to get script to run
- Browser or system crashes due to mishandling of resources
  - Temp/log file creation
  - Endless loops
  - Faulty use of APIs

Review Activity: Basics of Scripting

- Shell Scripts
- Basic Script Constructs
- Windows Scripts
- JavaScript and Python
- Use Cases for Scripting
- Scripting Best Practices and Considerations

Lab Activity

- Assisted Lab: Implement a PowerShell Script
  - Develop a PowerShell script to automate creation on virtual machines
- Assisted Lab: Implement a Bash Script
  - Develop a Bash script to automate gathering information from a Linux host

CompTIA A+ Core 2 Exam 220-1102

Lesson 19

Summary