2021 Cyber Security Academy - MTU June 8th - 11th
Can You Hack it?

Day 1: Lab 3
Windows Command Prompt and PowerShell

PowerShell Challenge 1: Aliases

- An important aspect to efficient PowerShell commands (and keystroke attacks – more on that Thursday) is the ability to identify aliases for commands.
- For example,
  - the “ls” command is an alias for “Get-ChildItem”.
- Task: Open PowerShell and enter:
  - “alias” to print the list of aliases.
  - Look through the list to identify the “Linux” commands.

- Enter: Get-Command explorer | Format-Table Path, Name

(This searches for the explorer.exe file and prints the path to that file)

- Enter: New-Item ExampleNewFile.txt
  - (This creates a new file)
- **Challenge** – Use available aliases to shorten those PowerShell commands.

Note: Aliases are critical for making efficient and optimized ethical keystroke injection attacks

PowerShell Challenge 2: My first PowerShell Script

- Switch to Windows 10 VM
- Start PowerShell.
  - Press Windows key
  - Type “PowerShell”
  - Double Click on “Windows PowerShell”
- Change directory to the Desktop (Hint use: cd)
- Create a new directory called “Scripts” on the Desktop by typing this command at the shell prompt:
  - mkdir Scripts
- Change to directory Scripts
- Use notepad to create a script file called hello.ps1:
  - notepad hello.ps1 (Click on Yes when asked if you want to create a new file.)

- Enter the following line at the top of the new file:
  - echo "Hello World!"
- Use the File menu to Save the file and then Exit notepad.
- In PowerShell Run the script: (make sure you are in the correct directory – Scripts)
  - ./hello.ps1
  - What is the output?
- Redirect the output of your script to a file called output.txt.
  - ./hello.ps1 > output.txt
- List the contents of the file:
  - cat output.txt
- **Can you write a second PowerShell script called make_file.ps1 that creates a New_file.txt and echo's "Hello World" to New_file.txt and prints the contents to the PowerShell command line?**
  - Hint: Remember Linux commands can be used e.g., touch, cat
  - Hint: Look at PowerShell Challenge 1
  - This can be done with three separate commands.

PowerShell/CMD Challenge 3: My first Linux Command

- Switch to Windows 10 VM
- Start Command Prompt cmd.exe
- Enter: Get-Command cmd | Format-Table Path, Name
  - Note the location of the cmd.exe file.
- Open notepad
- Write out the equivalent CMD command for the Linux command.
  - For example, pwd: @echo %cd%
  - save as pwd.cmd in C:\windows\system32\
- Open a new cmd.exe.
  - run pwd.

Challenge: Can you use this approach to make similar basic commands for "ls" & "cat"

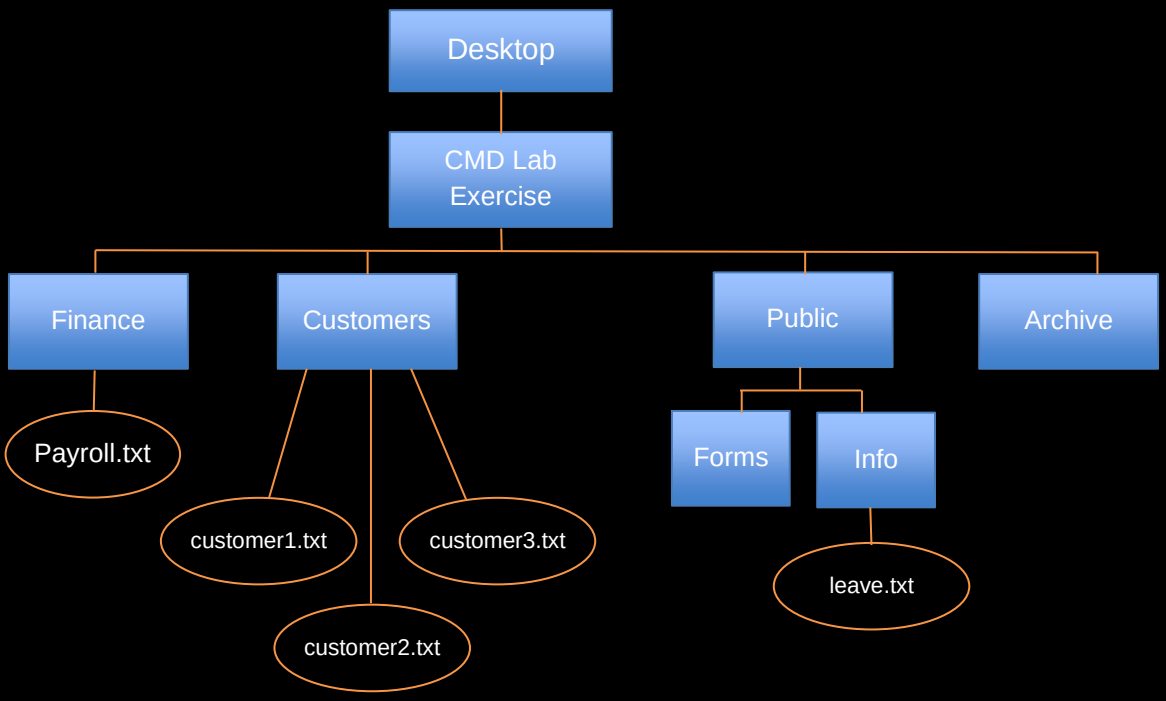
2021 Cyber Security Academy - MTU June 8th - 11th
Can You Hack it?

Challenge 4: CMD Lab - Practising your skills

Using the commands

- mkdir
- cd
- cd..
- move
- copy
- dir

create the following structure on your home directory, where the square boxes are folders, the lines represent folders (or files) contained inside each one. As per the diagram below, the structure looks like a hierarchy, and this is what the use of folders provides for – a hierarchy of where data should be saved and stored.



Before you start, using any application you like (e.g., Notepad or cmd.exe), create three text files: customer1.txt; customer2.txt and customer3.txt and two documents leave.txt and payroll.txt. These should be created and saved on your desktop.

Task: Implement the folder structure and write down the sequence of commands that you used.

2021 Cyber Security Academy - MTU June 8th - 11th
Can You Hack it?

Task: Now that you have created the directory structure, implement the following commands using the command prompt only.

1. Move the three customer files to the customer directory.
2. Copy the three customer files to the archive directory using a single command.
3. Copy the leave.txt file to the Info directory.
4. Move the payroll.txt file to the finance directory.
5. Move the file leave.txt to the archive directory and rename it leave_old.txt
6. Place leave_old.txt in the forms directory.
7. Change to the customer directory and check that it contains the three customer files.
8. Change to the archive directory and check it contains the three customer files that you copied.
9. Change back to the customer directory and delete the three customer files.

Additional Task for those who have a Windows personal machine.

PowerShell Extra Challenge: Blinking LED

- Start PowerShell.
- The following command will blink the CAPSLOCK key on your keyboard.
- $wsh = New-Object -ComObject WScript.Shell;$wsh.SendKeys('{CAPSLOCK}'); sleep -m 250;$wsh.SendKeys('{CAPSLOCK}');sleep -m 250;$wsh.SendKeys('{CAPSLOCK}');sleep -m 250;$wsh.SendKeys('{CAPSLOCK}');sleep -m 250;
- This is very useful for keystroke injection attacks as it can be used as a visual indicator of progress.

2021 Cyber Security Academy - MTU June 8th - 11th
Can You Hack it?

Java Installation

- For Thursday's USB Rubber Ducky Labs, you will need to have Java installed on your personal computer (Windows, MAC, Linux)
- This will allow you to encode the Rubber Ducky with the Payloads
- We will test the payloads on the Windows 10 VM, your personal machine is only required to encode the device (more on this on Thursday)
- Task 1: Install java
    - We can now use the USB Rubber Ducky Encoder GUI to encode the payloads.
- Task 2 (Optional): Add Java to your path
    - Use the PowerShell "Get-Command java | Format-Table Path, Name" command to find location of the java.exe file.
    - How do we add to path Windows?
        1. Open the Start Search, type in "env", and choose "Edit the system environment variables":
        2. Click the "Environment Variables…" button.
        3. Under the "System Variables" section (the lower half), find the row with "Path" in the first column, and click edit.
        4. The "Edit environment variable" UI will appear.
        5. Click "New" and add the java path from task 1.
        6. Click Ok and restart the CMD.exe