Blue Team Labs Online: PowerShell Analysis - Keylogger

The following writeup is for PowerShell Analysis - Keylogger on Blue Team Labs Online, it's an easy lab that involves analysing a suspicious PowerShell script. I honestly do not recommend this challenge as it is extremely easy and you honestly don't learn much.

Scenario: A suspicious PowerShell script was found on one of our endpoints. Can you work out what it does?

What is the SHA256 hash value for the PowerShell script file?

To generate the SHA256 hash, I am going to use the Get-FileHash PowerShell cmdlet:

```
PS C:\Users\vboxuser\Desktop > Get-FileHash -Algorithm SHA256 .\HDWallpaperEngine.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          E0B7A2AD2320AC32C262AEB6FE2C6C0D75449C6E34D0D18A531157C827B9754E       C:\Users\vboxuser\Desktop\HDWallpaperEngine.txt
```

What email address is used to send and receive emails?

```
PS C:\Users\vboxuser\Desktop > cat .\HDWallpaperEngine.txt | grep "@"
$From = "chaudhariparth454@gmail.com"
$To = "chaudhariparth454@gmail.com"
  $signatures = @'
'@
```

What is the password for this email account?

If we open up the text file using Notepad or some form of text editor, we can see the password being defined in the Pass variable:

```
$Pass = "yjghfdafsd5464562!"
```

What port is used for SMTP?

587:

```
$SMTPPort = "587"
```

What DLL is imported to help record keystrokes?

user32.dll:

```
[DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]
public static extern short GetAsyncKeyState(int virtualKeyCode);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int GetKeyboardState(byte[] keystate);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int MapVirtualKey(uint uCode, int uMapType);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
```

It is pretty obvious that this DLL is imported to record keystrokes due to the imported functions.

What directory is the generated txt file put in?

The temp directory:

```
function Start-KeyLogger($Path="$env:temp\keylogger.txt")
```