



UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE CIENCIAS FISICO MATEMATICAS



LABORATORIO DE PROGRAMACION PARA CIBERSEGURIDAD

Evidencia de practica #5: Scripting en PowerShell

Nombre: Brayan Osvaldo Ortiz Méndez

Matricula: 1912975

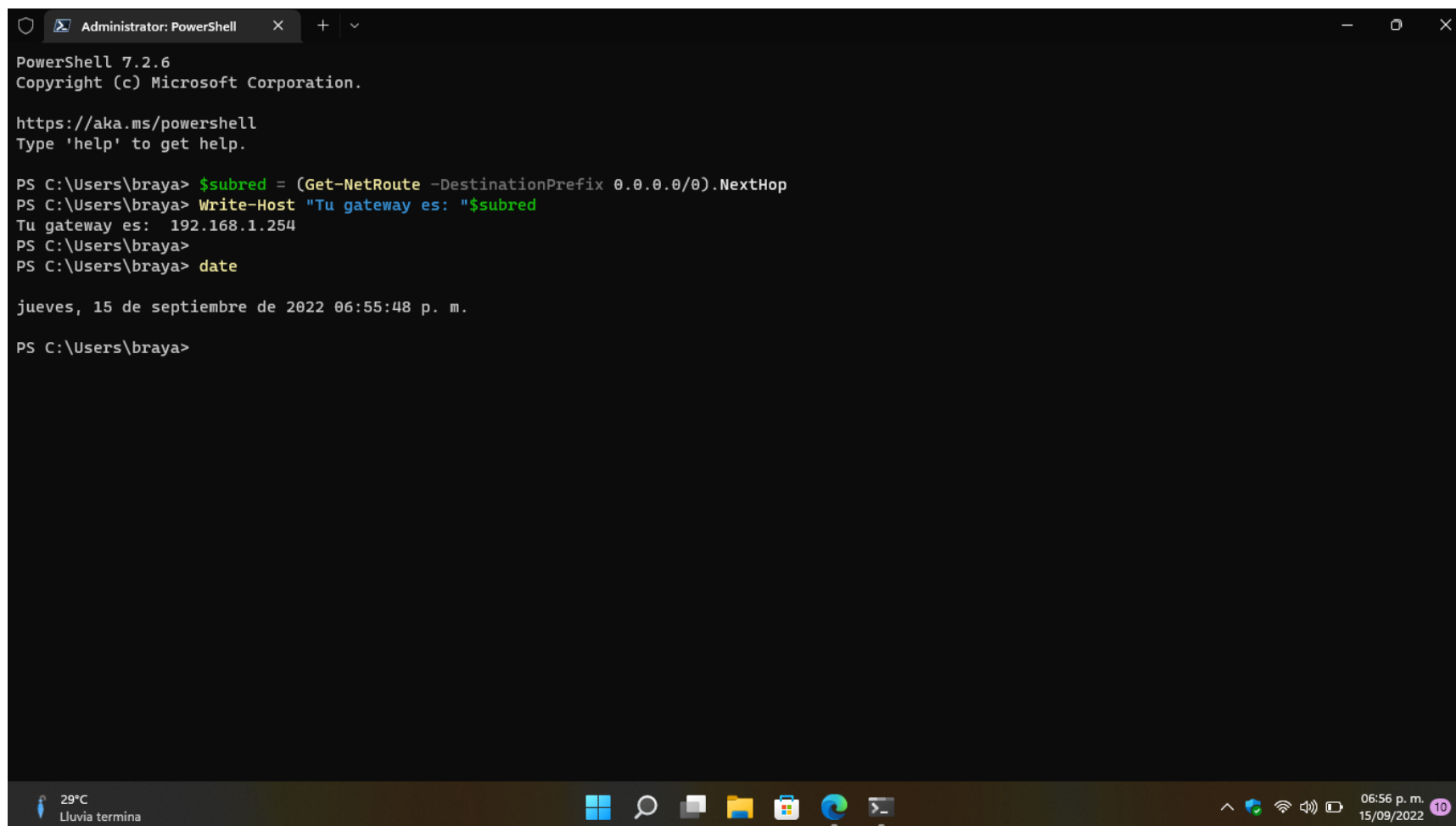
Grupo: 063

Maestro: Gerardo Bernal Carranza

Monterrey, Nuevo León

Jueves 15 de Septiembre del 2022

PARTE 1 - paso 1



```
Administrator: PowerShell
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS C:\Users\braya> $subred = (Get-NetRoute -DestinationPrefix 0.0.0.0/0).NextHop
PS C:\Users\braya> Write-Host "Tu gateway es: "$subred
Tu gateway es: 192.168.1.254
PS C:\Users\braya>
PS C:\Users\braya> date

jueves, 15 de septiembre de 2022 06:55:48 p. m.

PS C:\Users\braya>
```

The screenshot shows a Windows PowerShell terminal window titled "Administrator: PowerShell". The window displays the PowerShell version (7.2.6) and copyright information. It then shows the user running a command to retrieve the default gateway IP address using `Get-NetRoute` and displaying it with `Write-Host`. The output shows the gateway is 192.168.1.254. The user also runs the `date` command, which shows the current date and time as Thursday, September 15, 2022, at 6:55:48 PM. The Windows taskbar is visible at the bottom, showing the system clock as 06:56 PM on 15/09/2022.

PARTE 1 – paso 2

```
Administrator: PowerShell
PS C:\Users\braya> $rango = $subred.Substring(0,$subred.IndexOf('.') + 1 + $subred.Substring($subred.IndexOf('.') + 1).IndexOf('.') + 3)
PS C:\Users\braya> echo $rango
192.168.1.
PS C:\Users\braya>
PS C:\Users\braya> date

jueves, 15 de septiembre de 2022 06:58:56 p. m.

PS C:\Users\braya>
```

29°C
Lluvia termina

06:59 p. m.
15/09/2022

PARTE 2 – Ejecución de script scan_alive2.ps1

```
Administrator: PowerShell
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5> .\scan_alivev2.ps1
== Determinando tu gateway...
Tu gateway: 192.168.1.254
== Determinando tu rango de subred ...
192.168.1.

-- Subred actual:
Escaneando: 192.168.1.0/24

Host responde: 192.168.1.165
Host responde: 192.168.1.190
Host responde: 192.168.1.232
Host responde: 192.168.1.240
Host responde: 192.168.1.254
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5>
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5>
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5> date

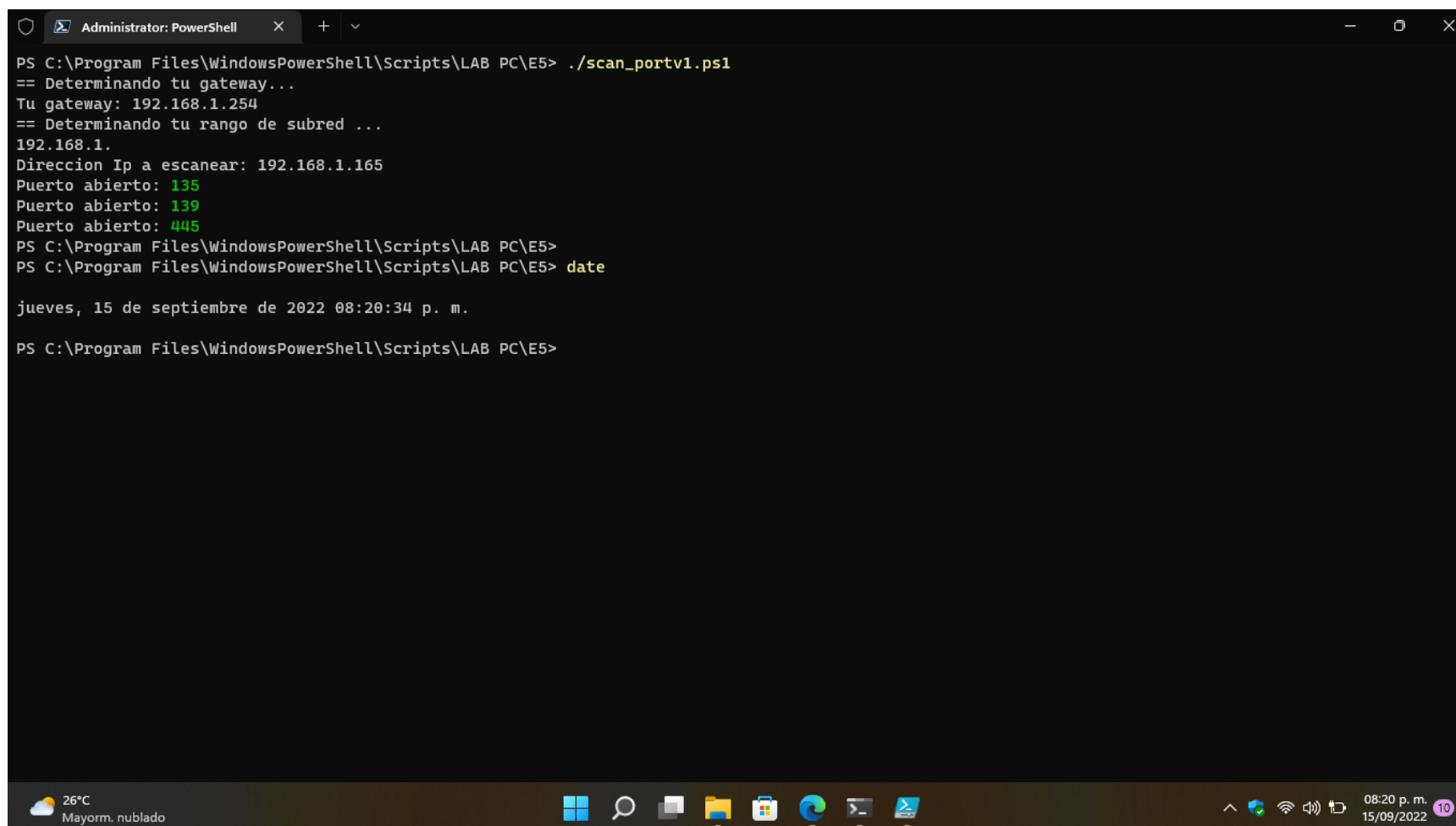
jueves, 15 de septiembre de 2022 07:56:23 p. m.

PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5>
```

26°C
Mayorm. nublado

07:56 p. m.
15/09/2022

PARTE 2 – Ejecución de script scan_portv1.ps1



The screenshot shows a Windows PowerShell terminal window titled "Administrator: PowerShell". The terminal displays the execution of a script named `scan_portv1.ps1` from the directory `C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5`. The script performs several actions: it determines the gateway (192.168.1.254), determines the subnet range (192.168.1), and scans for open ports on the IP 192.168.1.165. It identifies three open ports: 135, 139, and 445, which are highlighted in green. After the scan, the user enters the `date` command, and the terminal displays the current date and time: "jueves, 15 de septiembre de 2022 08:20:34 p. m.". The Windows taskbar at the bottom shows the system clock as 08:20 p. m. on 15/09/2022, along with weather information (26°C, Mayorm. nublado) and various system icons.

```
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5> ./scan_portv1.ps1
== Determinando tu gateway...
Tu gateway: 192.168.1.254
== Determinando tu rango de subred ...
192.168.1.
Direccion Ip a escanear: 192.168.1.165
Puerto abierto: 135
Puerto abierto: 139
Puerto abierto: 445
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5>
PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5> date

jueves, 15 de septiembre de 2022 08:20:34 p. m.

PS C:\Program Files\WindowsPowerShell\Scripts\LAB PC\E5>
```