

Useful Powershell Commands

Get Systemboot/Reboot/Shutdown Events

```
Get-EventLog System -Newest 10000 | `
    Where EventId -In 41,1074,1076,6005,6006,6008,6009,6013 | `
    Format-Table TimeGenerated,EventId,UserName,Message -AutoSize -Wrap
```

Ping with Timestamps

```
$target = "www.google.com"
ping -t $target | ForEach {"{0} - {1}" -f (Get-Date),$_}
```

Simple TCP Portscan

```
$target = "portquiz.net"
$firstport = 1
$lastport = 65535
for($port=$firstport; $port -le $lastport; $port++) {
    Test-NetConnection -ComputerName $target -Port $port
}
```

Packet Capture

Capture

```
$duration=90 $env:HostIP = (
```

```
Get-NetIPConfiguration |
Where-Object {
    $_.IPv4DefaultGateway -ne $null -and
    $_.NetAdapter.Status -ne "Disconnected"
}
```

```
).IPv4Address.IPAddress
```

```
netsh trace start capture=yes IPv4.Address=$env:HostIP tracefile=c:\temp\capture.etl Start-Sleep
$duration netsh trace stop
```

Convert to PCAP

<https://github.com/microsoft/etl2pcapng/releases>

```
https://github.com/microsoft/etl2pcapng/releases/download/v1.9.0/etl2pcapng.exe  
./etl2pcapng.exe c:\temp\capture.etl c:\temp\capture.pcap
```

Useful Commandlets

```
Format-Hex $filename
```

ActiveDirectory Commandlets/Scripts

Groups / GroupMembers

```
$file="C:\Temp\GroupCount.csv"  
Get-ADGroup -Filter * -Properties Member `\  
| Select-Object Name,@{n="MemberCount";e={$_.Member.Count}} `\  
| Export-Csv -Path $file -Delimiter '|'`
```

[kb](#), [windows](#), [powershell](#)

From:

<http://fortytwo.adurias.org/> - **Fortytwo - Answer to the Ultimate Question of Life, the Universe, and Everything**

Permanent link:

<http://fortytwo.adurias.org/powershell?rev=1668935947>

Last update: **2022/11/20 10:19**

