

Test1 – Entering IP address to end IP address range

```

112 # if IP responds to ping
113 if ($?Test-Connection -ComputerName $Target -Count 1 -Quiet)) {
114     Write-Host "Target is pingable."
115     # test if WS-MAN is enabled
116     if ($?Test-WSMAN -ComputerName $Target 2>$null)) {
117         Write-Host "`t WS-MAN is enabled"
118     } else {
119         Write-Host "`t WS-MAN is disabled"
120     }
121     # port scan
122     foreach ($port in $ports) {
123         Write-Progress -Activity "Scanning IP range" -Status $("Scanning " + $Target + ":" + $port) -PercentComplete $((($i/$Targets.Count)*100)
124         $socket = New-Object Net.Sockets.TcpClient # create new socket to connect
125         $ErrorActionPreference = 'SilentlyContinue'
126         $socket.Connect($Target,$port) 2>$null
127         $ErrorActionPreference = 'Continue'
128         if ($socket.Connected) {
129             "`t Port $port is open."
130             $socket.Close() # close socket
131         }
132         $socket.Dispose() # dispose of socket
133         $socket=$null

```

```

PS C:\WINDOWS\system32> C:\Users\Tees\Desktop\packet_code_samples\powershell_sweeps_and_scans\LOLscan.ps1
Enter the starting IP address: 192.168.56.100
Enter the last IP address or CIDR #: 192.168.56.102
192.168.56.100 is pingable.
WS-MAN is disabled
192.168.56.101 is pingable.
WS-MAN is disabled
Port 21 is open.
Port 22 is open.
Port 23 is open.
Port 80 is open.
Port 139 is open.
Port 445 is open.
PS C:\WINDOWS\system32>

```

Completed | Ln 57 Col 25 | 100%

Test2 – Entering CIDR notation to end IP address range

```

112 # if IP responds to ping
113 if ($?Test-Connection -ComputerName $Target -Count 1 -Quiet)) {
114     Write-Host "Target is pingable."
115     # test if WS-MAN is enabled
116     if ($?Test-WSMAN -ComputerName $Target 2>$null)) {
117         Write-Host "`t WS-MAN is enabled"
118     } else {
119         Write-Host "`t WS-MAN is disabled"
120     }
121     # port scan
122     foreach ($port in $ports) {
123         Write-Progress -Activity "Scanning IP range" -Status $("Scanning " + $Target + ":" + $port) -PercentComplete $((($i/$Targets.Count)*100)
124         $socket = New-Object Net.Sockets.TcpClient # create new socket to connect
125         $ErrorActionPreference = 'SilentlyContinue'
126         $socket.Connect($Target,$port) 2>$null

```

```

Scanning IP range.
Scanning 192.168.56.101:5985.

PS C:\WINDOWS\system32> C:\Users\Tees\Desktop\packet_code_samples\powershell_sweeps_and_scans\LOLscan.ps1
Enter the starting IP address: 192.168.56.1
Enter the last IP address or CIDR #: 255
192.168.56.1 is pingable.
WS-MAN is disabled
Port 139 is open.
Port 445 is open.
192.168.56.100 is pingable.
WS-MAN is disabled
192.168.56.101 is pingable.
WS-MAN is disabled
Port 21 is open.
Port 22 is open.
Port 23 is open.
Port 80 is open.
Port 139 is open.
Port 445 is open.

```

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger. | Ln 42 Col 1 | 100%