**Network Enumeration**

**List all network interfaces, IP, and DNS.**

ipconfig /all

Get-NetIPConfiguration | ft InterfaceAlias,InterfaceDescription,IPv4Address

Get-DnsClientServerAddress -AddressFamily IPv4 | ft

**List current routing table**

route print

Get-NetRoute -AddressFamily IPv4 | ft DestinationPrefix,NextHop,RouteMetric,ifIndex

**List the ARP table**

arp -A

Get-NetNeighbor -AddressFamily IPv4 | ft ifIndex,IPAddress,LinkLayerAddress,State

**List all current connections**

netstat -ano

**List firewall state and current configuration**

netsh advfirewall firewall dump

or

netsh firewall show state

netsh firewall show config

**List firewall's blocked ports**

$f=New-object -comObject HNetCfg.FwPolicy2;$f.rules | where {$\_.action -eq "0"} | select name,applicationname,localports

**Disable firewall**

netsh firewall set opmode disable

netsh advfirewall set allprofiles state off

**List all network shares**

net share

**SNMP Configuration**

reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s

Get-ChildItem -path HKLM:\SYSTEM\CurrentControlSet\Services\SNMP -Recurse