C:\> `netsh wlan set hostednetwork mode=allow ssid=<MYSSID> key=<MYPASSWORD> & netsh wlan start hostednetwork`

Configure a Windows machine as a WPA2-PSK Access Point.

Usage scenario: Share a Windows machine’s Internet access with other systems wirelessly, or use a Windows machine to attract wireless clients into joining it for exploitation purposes.

C:\> `netsh interface portproxy add v4tov6 listenport=<LPORT> listenaddress=0.0.0.0 connectport=<RPORT> connectaddress=<RHOST>`

Configure a TCP port forwarding relay from IPv4 to IPv6 (v4tov4, v6tov6, and v6tov4 also supported).

Usage scenario: Pivot a TCP connection through a Windows machine using built-in functionality, converting IPv4 to IPv6 as needed.

C:\> `netstat -naob 1 | find "<IPADDR or PORT>"`

Get a list of TCP and UDP activity every 1 second.

Usage scenario: Look for a connection coming in from a specific IP address or port to determine when the connection occurs, within 1 second.

C:\> `wmic process list full`

Get a list of all available attributes of all running processes.

Usage scenario: Look through processes to determine what is running, including potentially exploitable software, malware, and other tools.

C:\> `tasklist /svc`

Get a list of services running inside of each process.

Usage scenario: Look for running services that might be exploitable or running malware.

Subscribe to SANS GPWN Mailing List
https://lists.sans.org/mailman/listinfo/gpwn-list