Blue team field manual cont

**Get a list of services and disable or stop:**

C:\> sc query

C:\> sc config "<SERVICE NAME>" start= disabled

C:\> sc stop "<SERVICE NAME>"

C:\> wmic service where name='<SERVICE NAME>' call ChangeStartmode Disabled

**Show all rules:**

C:\> netsh advfirewall firewall show rule name=all

**Set firewall on/off:**

C:\> netsh advfirewall set currentprofile state on

C:\> netsh advfirewall set currentprofile firewallpolicy blockinboundalways, allowoutbound

C:\> netsh advfirewall set public profile state on

C:\> netsh advfirewall private profile state on

C:\> netsh advfirewall set domainprofile state on

C:\> netsh advfirewall set allprofile state on

C:\> netsh advfirewall set allprofile state off

**Set firewall rules examples**

C:\> netsh advfirewall firewall add rule name="OPEN Port 80" dir=in action=allow protocol=TCP localport=80

C:\> netsh advfirewall firewall add rule name="My Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes

**Change password:**

C:>\net user <USER NAME> \* /domain

C:\>net user <USER NAME> <NEW PASSWORD>

**SEND NTLMv2 response only/refuse LM and NTLM:**

C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ /v lmcompatabilitylevel /t REG\_DWORD /d 5 /f

**restrict anonymous access:**

C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ /v lmcompatabilityleve /t REG\_DWORD /d 5 /f

**do not allow anonymous enumeration of sam accounts and shares:**

C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v restrictanonymoussam /t REG\_DWORD /d 1 /f

**disable ipv6:**

C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v restrictanonymoussam /t REG\_DWORD /d 255 /f

**disable sticky keys:**

C:\> reg add "HKCU\ControlPanel\Accessibility\ToggleKeys" /v Flags /t REG\_SZ /d 58 /f

**disable toggle keys**

C:\> reg add "HKCU\ControlPanel\Accessbility\Keyboard Response" /v Flags /t REG\_SZ /d 122 /f

**disable filter keys:**

C:\> reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI /f /v ShowTabletKeyboard /t REG\_DWORD /d 0

**disabe onscreen keyboard**

C:\> reg add HKLM\**SYSTEM\CurrentControlSet\Control\Lsa /f /v NoLMHash /t REG\_DWORD /d 1**