Networking

Extract Wifi Keys
https://www.purehacking.com/blog/vitaly-nikolenko/extracting-wireless-wep/wpa/wpa2-preshared-keys/passwords-from-windows-7

ICMP Tunneling
icmpsrv & icmpsend
`icmpsrv --install` (on Victim)
`netstat -a` (icmpsrv should not show)
`icmpsend 192.168.1.8` (on Attacker, to connect to Victim)
Capture with Wireshark for more info

Hosts File
https://www.petri.com/easily-edit-hosts-file-windows-10
Copy from `C:\Windows\System32\Drivers\etc` to desktop then edit and copy back

Open URL from CMD without the Browser
http://stackoverflow.com/questions/20782734/open-a-url-without-using-a-browser-from-a-batch-file

WMIC GPUPDATE

```
Runas
/user:DOMAIN\domainadminuser "explorer /separate"
Wmic product list status
gpupdate /force
net user userid /domain
```

Processes

`fport` (to list pids, ports, protocols, exe)
`prcview.exe`
`tcpview.exe` (ports, exe, etc...)

CMD Tricks

WINKEY+R, `cmd /K dir` (run dir in cmd)
WINKEY+R, `cmd /C tree C:\` (run tree in cmd then close)
WINKEY+R, `cmd /C "start /MIN explorer \\x.x.x.x"`
WINKEY+R, `powershell Start-Process cmd -Verb runAs` (open cmd prompt as admin. hit ALT+Y to approve)
`start .` (open windows explorer in current dir)
`start /MIN .` (open explorer minimised)

Find Outlook PST Files

If a user has removed their pst files from outlook and has forgotten where they are located you can find them by editing the xml file below in notepad:
`C:\Documents and Settings\userid\Application Data\Microsoft\outlook\userid.xml`
Then look for instances of something like:
`<eidstore>00000000...6F74 646E6800</eidstore>`

Find Outlook PST Files (cont)

Copy and paste the HEX part (`0000000038A1BB1005E...E7 4732F636E3D6F74646E6800`) into a HEX to ASCII converter and it will show you the pst file location in plain-text.
Note: Sometimes the first 2 instances just show the exchange data. If that's the case just move onto the next HEX instance.

Psexec - Execute commands remotely

```
psexec \\x.x.x.x -u
DOMAIN\user -i 0 cmd.exe
/c "dir c:\ >
c:\temp\temp.txt"
psexec \\x.x.x.x -u
DOMAIN\user -i 0 cmd.exe
/c "start"
```

Giving Local Admin

Via a Domain Admin account
Right click on 'My Computer' -> Manage
Right click on "Computer Management (Local)" -> "Connect to another computer"
Type in Computer Name -> Press OK
System Tools -> Local Users and Groups -> Groups
Double click on "Administrators" -> Add
Click on Locations and then select their computer name
DOMAIN\username -> Press Ok

Hotkeys

WINKEY+R (Run)
ALT+F4 OR CTRL+SPACE C (Quit)
ALT+Y (Hit Yes)

Files & Directories

`tree c:\` (view in tree format)

Recover hard deleted items in Outlook

User has hard deleted an item (SHIFT+DEL) and cannot recover it using 'Recover deleted items'.
Full description = Microsoft KB246153.
Steps
1. Close Outlook
2. Start Registry Editor (Regedt32.exe).
3. Locate and click the following key in the registry:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client\Options
4. On the Edit menu, click Add Value, and then add the following registry value:
Value name: DumpsterAlwaysOn
Data type: DWORD
Value data: 1
5. Quit Registry Editor.
Start Outlook, click on folder (in folder view) which item was hard deleted from, select Recover Deleted Items from Tools menu and you should be able to recover items.