Internal Penetration Test (Active Directory Environments)
Unauthenticated Information Gathering
Automated Tools

☐ Generate nmap output files (with targets in targets.txt):
nmap -oA nmap-out -sV -p- -vv -iL targets.txt

☐ For tests with lots of web hosts, grab screenshots with a tool like aquatone

☐ Import nmap findings into Metasploit
create a new workspace workspace -a
import the file
db_import nmap-out.xml
view 5060 and 2000 to see if they are legit (they probably are not)
services -p 5060,2000
delete them
services -p 5060,2000 -d

☐ Use Metasploit modules for web dir/file enumeration
msfconsole
spool dir-scanner.txt
use auxiliary/scanner/http/dir_scanner
set DICTIONARY /opt/SecLists/Discovery/Web-Content/common.txt
services -u -p 80 --rhosts set rport 80
set ssl false
run
services -u -p 443 --rhosts set rport 443
set ssl true
run
repeat for other web ports (8443, 8080, etc)

☐ Check for anonymous SMB shares with auxiliary/scanner/smb/smb_enumshares.

☐ Check for open NFS shares with auxiliary/scanner/nfs/nfsmount.

☐ Check for anonymous FTP shares with auxiliary/scanner/ftp/anonymous.

☐ Create a list of machines that are not configured to do SMB signing (for relaying later on).

- ☐ crackmapexec '--gen-relay-list'

Manual Review

- ☐ Identify all URLs that allow logins.
- ☐ Manually review screenshots from all HTTP services.

Obtaining Credentials

- ☐ Responder attack.
  - ☐ First, run in analyze mode. Determine blue-teamy stuff and then run configure Responder.conf to not respond to those IPs.
- ☐ Execute an ipv6 mitm attack.
- ☐ Getting action from standard responder or mitm6? Use Impacket's ntlmrelay.py to dump SAM and/or get interactive SMB shells.
- ☐ Start cracking any received challenge/response data.
- ☐ Wireless WPA-Enterprise attacks to gather usernames, hashes, and passwords.
  - ☐ airgeddon is a nice automation tool for hostapd-wpe.
- ☐ Find any printer admin pages? Try default creds and look for LDAP integration.
- ☐ Drop a few USB sticks in the conference rooms (don't push the scope!).
- ☐ Internal password spray:
  - ☐ Metasploit's auxiliary/scanner/smb/smb_login.
  - ☐ CrackMapExec.

Authenticated Information Gathering

- ☐ Manually review scripts in \\domain_name\netlogon
  - ☐ Don't just look for passwords - look for references to dev environments, deployment servers, etc.
- ☐ Run the Sharphound injestor and map paths in Bloodhound.
- ☐ Enumerate shares with crackmapexec '--shares'
- ☐ Rummage through shares.
- ☐ Rummage through Sharepoint, e-mail, etc.
  - ☐ Look for anything related to new accounts and passwords resets. IT often uses standard passwords for these. If you find one, spray it around.
- ☐ Enumerate and map network connectivity with a tool like leprechaun.

Initial Foothold

☐ [ ]

Local Privilege Escalation

☐ Try WindowsEnum or similar script to cover the basics.
☐ Use a test machine to observe procmon.exe for vendor 0-days (writable DLL and service paths, etc)

Domain Privilege Escalation

☐ Get SPNs (Kerberoast - get that GPU humming!)
☐ Run Grouper
☐ Running SQL servers? Try for authenticated SQL/SMB relay with auxiliary/admin/mssql/mssql_ntlm_stealer
☐ Leverage existing credentials to get more credentials or passable hashes.
- ☐ crackmapexec '--sam'
- ☐ crackmapexec '--lsa'
- ☐ crackmapexec '-M mimikatz'
- ☐ Windows Task Manager or procdump.exe to dump lsass and use mimikatz or pypykatz

☐ Find logged in users and sessions on boxes you have admin rights to.
- ☐ crackmapexec '--loggedon-users'
- ☐ crackmapexec '--sessions'

☐ Review Bloodhound path's to DA with:
- ☐ All currently compromised accounts
- ☐ All logged-on users on boxes you have admin rights to

Objective Hunting

☐ Use Impacket's secretsdump.py to access credentials for specific accounts you need.