External Penetration Test
Mapping Attack Surface
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)
```

Manual Review

☐ Identify all URLs that allow logins from Spiderfoot.

☐ Review all the discovered URLs from the Metasploit dir scanners.

☐ Identify all systems that may provide remote access (Citrix, RDP, VPN, etc).

☐ Identify all vendor-products that are likely to offer RCE-as-a-feature (Jenkins, Serv-U, etc).

☐ Identify all vendor products that may allow you to download a trial version to look for 0-days.

Obtaining Credentials

Password Spraying

☐ Make damn sure you know the lockout policy you are up against.

☐ Do you have reliable username enumeration on an endpoint? OWA, Skype, etc.

- ☐ If so, do a fine-tuned first run with usernames from OSINT phase PLUS as much from the likely usernames as you have time for.

☐ Spray a service accounts list like this one with username-as-password.

☐ Spray your known-good corporate usernames against common passwords, staying safely below lockout rates.

- ☐ The classics
- ☐ SeasonYear (Summer2019)
- ☐ MonthYear (March2019)
- ☐ CompanyNumber (Google1)
- ☐ CompanyYear (Google2019)
- ☐ ^^ All of the above without a capital first letter, and a ! at the end (still meets complexity requirements)
- ☐ ^^ All of the above with a ! at the end.
- ☐ No luck? Get creative with things like the corporate HQ address, corporate mottos, etc.

☐ Still no creds and safe to try more without locking out? Try weak passwords based on company name, location, etc.

Authenticated Information Gathering

☐ Gather all user accounts from:
- ☐ OWA or Office365 address list
- ☐ portal.azure.com (Azure AD)
- ☐ Lync (Windows app will download and cache the GAL locally)

☐ Search email inboxes for:
- ☐ "Password" - look for standard password IT uses to reset
- ☐ "Remote Access" - look for info on connecting to VPN, etc
- ☐ "Intranet", "Portal", "HelpDesk", etc - look for sources of internal company info

☐ Hang out in company chat rooms in Slack, Skype, etc.

☐ Check calendars for dial in info for board meetings and other sensitive events.

☐ Check Office365, Sharepoint, Drive, etc for similar sensitive details.

☐ Try additional password spraying with new accounts and likely passwords you have gathered.

Breaching the Perimeter

☐ Leverage all available remote access services, such as:
- ☐ RDP
- ☐ Citrix
- ☐ VPN

☐ Identified any RCE-by-design apps during OSINT? Try the credentials on those.

☐ Look for trial versions of any off-the-shelf applications on perimeter, download, find 0 days.