PWNAGE CHECKLIST

* establish vpn connectivity / confirm connectivity
* check my ip
* scan target network
  + basic ping sweep on large range
  + select target – make note of ip in evernote
  + document everything
* indepth nmap scan
  + NMAP -SC -SV -O -T2/3 IP-TARGET -V
    - SAFE SCRIPTS, SERVICE DISCOVERY, OS DETECTION, SLOWER SCAN (TO BE SAFE), VERBOSE
* IF PORT 80 / 443 OPEN
  + nikto -h ip-target
  + DIRB <HTTP://IP-TARGET> -R
    - NON-RECURSIVE TO SAVE TIME
  + PERHAPS NMAP –SCRIPT –HTTP-ENUM
  + CHECK SITE IN BROWSER
    - RESOLVE HOSTNAME IF NEEDED (ETC/HOSTS)
    - CHECK SOURCE
      * LOOK FOR DIRECTORIES
      * COMMENTS
      * SCRIPT LINKS
      * FORM METHODS
      * LOGIN FORMS
        + SEE IF THERES VERSION NUMBERS OR SOFTWARE NAMES
        + TRY BASIC SQL INJECTION
* open PORTs
  + nmap enumerate if possible with scripts if nothing came up before. perhaps change scan speed to slower one
  + enum4linux
  + smbclient
    - smbclient \\\\ip\\share
  + try to connect to them to see if they are truly alive
    - ssh ip-target
    - ftp root@ip-target etc
    - check for version numbers
      * use searchsploit / google for known vulns
* find writeable directories if /tmp or /dev/shm not available
  + find / -type d \( -perm -g+w -or -perm -o+w \) -exec ls -adl {} \;
* netcat
  + > output to a file
  + nc target-ip port < send from kali
* upgrade linux shell
  + python -c “import pty; pty.spawn(‘/bin/bash’)”
    - ctrl+z backgrounds the shell on local box
    - then type:
      * ssty raw -echo
      * fg
      * reset
    - if size is an issue type:
      * stty size (returns current window size)
      * stty -rows 48 -columns 120 (eg size)
* priv esc linux
  + try sudo su or sudo -l
  + if these don’t work try get kernel and distro info to look for exploits
    - uname -ar
    - cat /etc/issue
    - cat /etc/\*-release
    - cat /etc/lsb-release
    - cat /etc/redhat-release

usefull links

<https://netsec.ws/?p=331> - msfvenom,shells,tips

<https://medium.com/@hakluke/haklukes-ultimate-oscp-guide-part-3-practical-hacking-tips-and-tricks-c38486f5fc97>