Miscellaneous Notes

Use this when you find yourself stuck, out of ideas, or in a rabbit hole.

Step 1: Relax, take a 10 minute break.

Step 2: Read through the following and see which applies to your situation.

See PGP Sybaris for Redis CLI, vault pgp for responder use in case of client side attacks, dibble for node, Butch for blind sqli

See thm room for guide on pivoting.

See the lateral pass in hpb 2 for lateral movement

Use NMAP automator for nmap.

For potato attacks, make sure to try all of them.

When testing for sql injection, try all queries to see which works- make sure to test writing data rather than just reading it

Always use the largest directory for web bruteforcing, and always try multiple tools. ferox, dirb, go, and wfuzz

Revert the scan if the port scan doesnt find anything

If on web, use multiple wordlists if you find nothing on a web server. no reason for it to be active if its not going to serve something. Feel free to try all the wordlists

If nothing found, make sure nmap did a full port scan by connecting to each port indivdually using a manual scanner

If you have a username, attempt SSH brute force

When using a new tool, make sure to see it's example usage to make sure you are using it correctly

If you can download, then you can upload. Always upload a shell or an SSH key

If you want to run something like connect to a database, or run SMB from local machine to copy files onto the target, use impacket's services

Always run all commands with sudo

Windows Priv ESC technique: with seimpersonateprivilege set, a windows 10 and 2016/2019 server can be escalated with printspoofer.

ALWAYS READ YOUR EXPLOIT CODE

Use ltrace to see the libraries used in running a command process in Linux in order to see if any those processes can be injected

Check SSL certs for virtual subdomains

Use 'bash -c "CMD"' with a URL encoded command to get a reverse shell

SSH tips
SSH bad keys repository
Brute force using custom data from Cewl and hydra or even rockyou if you have a username
Patator for fuzzing
Crowbar for key brute forcing
Metasploits SSH login

Use individual enumerators for CMS

Study simpler web stuff, courses on bug bounties

Use ping to test for rce. Set ping as the command, and use wireshark or tcpdump to watch the ping hit your machine

Always install CMS or webservers to check for config file locations.

Updated Linux exploit suggester and windows exploit suggester

Rce to shell instructions: step 1, use ping to test rce. Step 2 Download NC or shell executable. Step 3 run NC or executable to get shell

When running an exploit, read it entirely to see if it works. Manually attempt parts of it. To confirm that it is the intended part. Then try all inputs multiple times, including URL, especially URL.

For privesc, check SQL databases for credentials

Write a script to run the following nmap scan against a machine: quick, full, vuln and enum for each port individually. After the quick scan, start exploring each thing on your own

Always guess credentials

Make a word list for directories that combines everything

Use already open common ports like 80 and 21 to transfer files as they are less likely to be blocked by firewalls. I.e. start a web server on local host and have it serve on the common port. Also run revshells over common ports

For webshells, use the web port

Use eot technique to write to files via tty

Use evilwinrm or psexec as SSH alternative for Windows

To fuzz webdomains for vhosts, see oxdf on htb sneaky mailer

For blind rce, use http to download a file to a certain folder. /tmp/exploit/ then change its execution policy, then run it via the blind rce.

Revshells: https://robertscocca.medium.com/%EF%B8%8F%EF%B8%8F-rce-to-shell-techniques-696e55b23fee

For certutil to download a reverse shell:

https://3895052089-files.gitbook.io/~/files/v0/b/gitbook-x-prod.appspot.com/o/spaces%2F-MFlgUPYI8q83vG2IJpI%2Fuploads%2Fgit-blob-0ecdbcc6b97e2898c2aa9776b689c4f38729051c%2Fimage.png?alt=media