Linux Checklist:

Adriel Plan:

- Use Web info to get way in – comb machines looking for misconfigs and priv esc vectors
- LinPEAS for low hanging fruit & hint or two of where to go
- FFUF, Hashcat
- When you get in through a service, you try to look for permissive services, files containing credentials (they're usually the config files for the service or a database)

Tools:

- ☐ LinPEAS

System Info:

- ☐ Get OS info
- ☐ Check path – any writable folder?
- ☐ Check env variables, any sensitive detail?
- ☐ Search for kernel exploits using scripts (Dirty Cow?)
- ☐ Check if sudo version is vulnerable
- ☐ Dmesg signature verification failed
- ☐ More system enum
- ☐ Date, system stats, CPU info, printers
- ☐ Enumerate more defenses

Drives

- ☐ List mounted drives
- ☐ Any unmounted drive?
- ☐ Any creds in fstab?

Installed Software

- ☐ Check for useful / vulnerable software installed

Processes

- ☐ Any unknown software running
- ☐ Any software with more privileges than it should have?
- ☐ Search for exploits of running processes (especially version running)

- ☐ Can you modify the binary of any running process?
- ☐ Monitor processes and check if any interesting process is running frequently
- ☐ Can you read interest process memory (where passwords can be saved)

Scheduled/Cron Jobs

- ☐ Is the PATH being modified by some cron jobs and can you write in it?
- ☐ Any wildcard in a cron job?
- ☐ Some modifiable script is being executed or inside a modifiable folder?
- ☐ Have you detected that some script could be or is being executed frequently? (every 1 2 5 min)

Services:

- ☐ Any writable .service file?
- ☐ Any writable binary executed by a service?
- ☐ Any writable folder in systemd PATH?

Timers

- ☐ Any writable timer?

Sockets

- ☐ Any writable .socket file?
- ☐ Can you communicate with any socket?
- ☐ HTTP sockets with interesting info?

D-Bus

- ☐ Can you communicate with any D-Bus?

Network

- ☐ Enumerate the network to know where you are
- ☐ Open ports you couldn't access before getting a shell in the machine?
- ☐ Sniff traffic with tcpdump

Users

- ☐ Generic users/groups enumeration
- ☐ Very big UID? Is the machine vulnerable?
- ☐ Can you escalate privs due to a group you're in?
- ☐ Clipboard data?
- ☐ Password Policy

- [ ] Try to use every known password that you have discovered previously to login with each possible user
- [ ] Try to login also without a password

Writable PATH

- [ ] If you have write privileges over some folder in PATH you may be able to escalate privileges

SUDO and SUID Commands

- [ ] Can you execute any command with sudo? Can you use it to READ, WRITE or EXECUTE anything as root? (GTFOBins)
- [ ] Is any exploitable SUID binary? (GTFOBins)
- [ ] Are sudo commands limited by path? can you bypass the restrictions?
- [ ] Sudo/SUID binary without path indicated?
- [ ] SUID binary specifying path? Bypass
- [ ] LD_PRELOAD vuln
- [ ] Lack of .so library in SUID binary from a writable folder?
- [ ] SUDO tokens available? Can you create a SUDO token?
- [ ] Can you read or modify sudoers files?
- [ ] Can you modify /etc/ld.so.conf.d/?
- [ ] OpenBSD DOAS command

Capabilities

- [ ] Has any binary any unexpected capability?

ACLs

- [ ] Has any file any unexpected ACL?

Open Shell Sessions

- [ ] screen
- [ ] tmux

SSH

- [ ] Debian OpenSSL Predictable PRNG - CVE-2008-0166
- [ ] SSH Interesting configuration values

Interesting Files

- [ ] Profile files – read sensitive data? Write to privesc?
- [ ] passwd/shadow files? – read sensitive data? write to privesc?

- ☐ Check commonly interesting folders for sensitive data
- ☐ Weird Location/Owned Files, you may have access to or alter executable files
- ☐ Modified in last mins
- ☐ Sqlite DB files
- ☐ Hidden files
- ☐ Script/binaries in PATH
- ☐ Web files (passwords?)
- ☐ Backups?
- ☐ Known files that contains passwords: Use Linpeas and LaZagne
- ☐ Generic search

Writable Files

- ☐ Modify python library to execute arbitrary commands?
- ☐ Can you modify log files? Logtotten exploit
- ☐ Can you modify /etc/sysconfig/network-scripts/? Centos/Redhat exploit
- ☐ Can you write in ini, int.d, systemd or rc.d files?

Other Tricks

- ☐ Can you abuse NFS to escalate privileges?
- ☐ Do you need to escape from a restrictive shell?

Links from Last Yr:
Linux PrivEsc Guide:
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md

GTFOBins:
https://gtfobins.github.io/