☑	Linux Privilege Escalation checklist	Information
☐	Credential re-use	Anything from earlier we can re-use?
☐	Check /var/www/html	Any hidden or config files on the webserver we can loot
☐	ls -la ~/	Any hidden files in home directory
☐	id;who;w;last;cat /etc/sudoers;cat /etc/group	Check information about the users on the box
☐	sudo -l	Check what you can run with sudo (are you even in sudoers) anything we can abuse?
☐	sudo su	Can we just sudo su?
☐	find / -perm -u=s -type f 2>/dev/null	Find all SUID's (without automated scripts)
☐	cat /etc/passwd ; cat /etc/shadow	Can we view passwd or shadow?
☐	netstat -antup	Any open ports on localhost we didnt see with nmap?
☐	ls -la /etc/cron.d	Check cron jobs
☐	ps aux	grep root	Either running as root or another user, maybe something running we can exploit	CHECK https://gtfobins.github.io/
☐	./linenum.sh > linenum-output.txt	wget/curl from localhost w/ python temp server https://github.com/rebootuser/LinEnum
☐	python linuxprivchecker.py > pychecker-out.txt	https://github.com/sleventyeleven/linuxprivchecker/blob/master/linuxprivchecker.py
☐	./unix-privesc-check > monkey-out.txt	http://pentestmonkey.net/tools/audit/unix-privesc-check
☐	uname -r ; cat /proc/version	Check kernel version searchsploit linux kernel xxx --exclude="(PoC)|/dos/"
☐	cat /home/*/.ssh/id_rsa	Grab ssh keys
☐	cat /root/proof.txt ; /sbin/ipconfig ; whoami;id	Grab proof.txt, ipconfig, and current user info