Άσκηση 8

Μπουρίτης Ιωάννης: 2021030173
Χατζάκης Εμμανουήλ-Θωμάς: 2021030061

1.

Η αδυναμία του **Greeter.c** βρίσκεται στη χρήση της συνάρτησης **gets()**. Επειδή δεν υπάρχει έλεγχος για το μέγεθος του input από τον χρήστη μπορούμε να κάνουμε overflow τον buffer με κατάλληλο input και να αλλάξουμε την τιμή της μεταβλητής Grade απο 6 σε 9. Για να γίνει το παραπάνω υλοποιήθηκε ένα python script (**change_Grade.py**) το οποίο γεμίζει τον buffer με μία ακολουθία από **A** και τον αριθμό 9 σε little endian (**\x09\x00\x00\x00**) όπου χρησιμοποιεί η αρχιτεκτονική x86. Ο λόγος που δεν γίνεται να αλλάξει ο βαθμός σε 10 είναι λόγω της λειτουργίας της **gets()** και της αναπαράστασης του 10 σε little endian (**\x0A\x00\x00\x00)**. Η συνάρτηση **gets()** σταματάει να λαμβάνει input όταν διαβάσει new line η οποία αναπαρίσταται ως **\x0A.**

2.

Για να εμφανίσουμε ένα τερματικό κατά την διάρκεια εκτέλεσης του κώδικα του **Greeter.c** πρέπει να αλλάξουμε την διεύθυνση επιστροφής της **readString()** και να τοποθετήσουμε σε κάποιο μέρος το python script του shellcode ώστε να εκτελεστεί.
Για να πραγματοποιήσουμε τα παραπάνω χρησιμοποιούμε τον gdb. Τοποθετούνται δύο breakpoints στη γραμμή που καλείται η συνάρτηση **readString()** και στο τέλος της. Γίνεται εκκίνηση του debugging με την εντολή **run** ή **r.** Στο πρώτο breakpoint με τη εντολή **p &buf** βρίσκεται η διεύθυνση του buf (**0xffffcd28)** και με την εντολή **p &Name** (**0x80ef320**) η διεύθυνση του πίνακα **Name** όπου θέλουμε να γυρίσουμε ώστε να εκτελέσουμε το script. Ο λόγος που εκτελούμε το script μέσο της **Name** είναι η χρήση του

flag **PROT_EXEC** που επιτρέπει στη **Name** να έχει εκτελέσιμο κώδικα μηχανής.

```
(gdb) p &buf
$1 = (char (*)[32]) 0xffffcd28
(gdb) p &Name
$2 = (unsigned char (*)[1024]) 0x80ef320 <Name>
```

Στο δεύτερο breakpoint με τη εντολή info frame βρίσκουμε το return address της readString (**eip: 0xffffcd5c**). Η αρχή του buffer μέχρι το return address είναι 52 bytes τα οποία τα γεμίζουμε με 28 bytes του shellcode 20 bytes με εντολές NOP και 4 bytes με τη διεύθυνση **0x80ef320.**

```
(gdb) info frame
Stack level 0, frame at 0xffffcd60:
 eip = 0x8049814 in readString (Greeter.c:29); saved eip = 0x804988a
 called by frame at 0xffffcd80
 source language c.
 Arglist at 0xffffcd58, args:
 Locals at 0xffffcd58, Previous frame's sp is 0xffffcd60
 Saved registers:
  ebp at 0xffffcd58, eip at 0xffffcd5c
```

Οι εντολές που εισάγουμε στο τερματικό για να γίνει η ‘επίθεση’ είναι:

1. python terminal.py, ώστε να εκτελεστεί το script και να δημιουργηθεί το αρχείο από όπου θα εισάγουμε το payload. Το αρχείο έχει όνομα payload_input.
2. (cat payload_input; cat) | ./Greeter, ώστε να εκτελεστεί το shell, έχει τοποθετηθεί και δεύτερη εντολή cat ώστε να παραμείνει ανοιχτός ο file descriptor του pipe και να έχουμε επαφή με το shell.