

Buffer Overflows

Ο στόχος της άσκησης αυτής, είναι να εκμεταλλευτείτε μια αδυναμία buffer overflow ενός εκτελέσιμου έτσι ώστε να αποκτήσετε πρόσβαση σε ένα αρχείο στο οποίο δεν έχετε δικαιώματα. Η άσκηση είναι **ατομική**.

Αρχικά, στο email που θα σας αποσταλεί με θέμα "**Project 2: BO**", θα σας δίνονται οι πληροφορίες που χρειάζεστε για να συνδεθείτε μέσω ssh σε έναν συγκεκριμένο εξυπηρετητή. Στο home directory σας θα βρείτε ένα εκτελέσιμο που λέγεται "**securelog**". Το πρόγραμμα αυτό ανήκει στον χρήστη "**t_{your_username}**" ($t \rightarrow$ target, συν το username σας) και χρησιμοποιείται, για την καταγραφή μηνυμάτων σε ένα αρχείο στο οποίο μόνο ο $t_{your_username}$ έχει πρόσβαση. Η χρήση του εκτελέσιμου είναι η ακόλουθη:

```
./securelog <YYYY-mm-ddTHH:MM:SS>_<message>
```

Θα πρέπει να εκμεταλλευτείτε την αδυναμία που υπάρχει στο εκτελέσιμο έτσι ώστε να μπορέσετε να αποκτήσετε πρόσβαση στο αρχείο. Επιπλέον, θα πρέπει να καλύψετε τα ίχνη σας έτσι ώστε ο $t_{your_username}$ να μην αντιληφθεί πως εσείς προσπαθήσατε και πετύχατε να δείτε τα περιεχόμενα του.

Στο home directory σας θα βρείτε ακόμα τα εξής αρχεία:

1. το `securelog.c`,
2. το `shellcode.txt` που χρειάζεστε για να εκτελέσετε εντολές ως $t_{your_username}$ και
3. το αρχείο `secure.log`.

Θα πρέπει να μελετήσετε πολύ προσεκτικά το `securelog.c` για να καταλάβετε ακριβώς πως λειτουργεί το εκτελέσιμο στο οποίο υπάρχει η ευπάθεια. Μπορείτε επίσης να κάνετε `compile` το αρχείο αυτό και να εξετάσετε το αντίστοιχο εκτελέσιμο που εκτός από την ίδια συμπεριφορά, θα χρησιμοποιεί διευθύνσεις μνήμης που θα βρίσκονται πολύ κοντά σε αυτές του original `securelog`. Στην περίπτωση που το κάνετε `compile` χρειάζεστε συγκεκριμένα `flags`:

```
gcc -g -ggdb -z execstack -fno-stack-protector -o my_securelog securelog.c
```

Εξετάζοντας το `shellcode.txt` θα παρατηρήσετε πως υπάρχει στο τέλος μια κλήση σε ένα αρχείο με το όνομα "**shell**". Αυτό σας επιτρέπει να φτιάξετε ένα εκτελέσιμο με το όνομα `shell`, το οποίο με τη σειρά του θα κάνει ότι θέλετε (λ.χ. να ανοίγει ένα shell). Το αρχείο `secure.log` είναι το αρχείο στο οποίο θέλετε να αποκτήσετε πρόσβαση. Προσοχή, **μην** σβήσετε το αρχείο αυτό. Σε αυτή την περίπτωση δεν θα μπορείτε να κάνετε την άσκηση.

Πρέπει να παραδώσετε μια αναφορά (report) στο csec.uoa@gmail.com μέχρι τις 30/05/2018 και ώρα 23:59. Στην αναφορά πρέπει να **εξηγήσετε** πως κάνατε την επίθεση (βήματα, την ευπάθεια που ανακαλύψατε, κώδικα που γράψατε, utilities που χρησιμοποιήσατε λ.χ. `gdb`). Επιπλέον θα πρέπει να αναφέρετε τα **περιεχόμενα** του αρχείου στην περίπτωση που καταφέρετε να αποκτήσετε πρόσβαση αλλά και πως καλύψατε τα ίχνη σας.

Εξώφυλλο Project: Το εξώφυλλο του project σας πρέπει να περιέχει τα ονόματά σας, τα ΑΜ σας, καθώς και τα στοιχεία "**Project #2**", "**ΥΣ13 ΕΑΡΙΝΟ 2018**".

Σημείωση: Στην περίπτωση που δημιουργήσετε νέα αρχεία **δικά σας**, φροντίστε να ορίσετε σωστά τα permissions ώστε να έχετε μόνο εσείς πρόσβαση σε αυτά. Θα μπορούσατε να το κάνετε αυτό για

όλο το directory σας **αλλά** κάτι τέτοιο δεν θα σας επέτρεπε να λύσετε την άσκηση! Το γιατί θα πρέπει να το αναφέρετε στο report.

Σημείωση 2: Το άρθρο "Smashing the Stack for Fun and Profit" του Aleph One (<http://insecure.org/stf/smashstack.html>), μπορεί να σας φανεί χρήσιμο για την επίλυση του project. Δείτε επίσης και το "Real and Effective IDs" (<http://www.makelinux.net/alp/083>).