Πανεπιστήμιο Αθηνών	Εαρινό 2014
ΥΣ13 Ασφάλεια Υπολογιστικών Συστημάτων	ΚΙΑΓΙΑΣ
Due: 23.05.2014	Project #1

Buffer Overflows

Ο στόχος του πρώτου project είναι να αποκτήσετε πρόσβαση στους λογαριασμούς άλλων χρηστών σε ένα υπολογιστικό σύστημα. Συγκεκριμένα το σύστημα που θα χρησιμοποιήσουμε τρέχει LINUX και βρίσκεται στη διεύθυνση `sbox.di.uoa.gr`. Μόνο το `ssh` είναι διαθέσιμο για να έχετε πρόσβαση στο σύστημα. Τα στοιχεία του λογαριασμού σας θα είναι σαν username το όνομα χρήστη που είναι στο πανεπιστημιακό σας e-mail (στις περισσότερες των περιπτώσεων ξεκινάει με ``sdi"). Το αρχικό σας password θα σας σταλεί με e-mail. Απαραίτητη προυπόθεση για να πάρετε λογαριασμό στο σύστημα sbox είναι να γραφτείτε στο forum της τάξης : `http://compsec.di.uoa.gr` με τον ενδεδειγμένο τρόπο και να χρησιμοποιήσετε το πανεπιστημιακό σας e-mail σαν contact information.

1. Στο συγκεκριμένο σύστημα πέρα από τους δικούς σας λογαριασμούς υπάρχουν και τρεις ακόμη: `superuser`, `hyperuser`, `masteruser`. Καθένας από αυτούς τους λογαριασμούς έχει ένα εκτελέσιμο αρχείο στον κατάλογο του με το `suid` bit ενεργοποιημένο (όλοι οι κατάλογοι των χρηστών είναι στον υποκατάλογο `/home/`). Σε όλες τις περιπτώσεις το εκτελέσιμο είναι μια απλή simple command-line utility. Σε κάποιες περιπτώσεις θα βρείτε και των κώδικα που αντιστοιχεί στο εκτελέσιμο ή κάποιες οδηγίες χρήσης (αλλα όχι σε όλες). Μαζί με αυτά τα αρχεία στον κατάλογο των τριών χρηστών υπάρχει και ένα μυστικό αρχείο το οποίο είναι προσπελάσιμο μόνο από τον ιδιοκτήτη του καταλόγου. Υπάρχουν τρία τέτοια αρχεία σε σύνολο `supersecret`, `hypersecret`, `mastersecret`.

2. Όλα τα εκτελέσιμα έχουν μια buffer overflow αδυναμία. Η αδυναμία είναι είτε εξαιτίας κακού κώδικα είτε εξαιτίας κακής επιλογής συναρτήσεων. Ο στόχος είναι να ανακαλύψετε την αδυναμία και τον τρόπο να την εκμεταλευτείτε ώστε να μπορέσετε να διαβάσετε τα μυστικά αρχεία των τριών χρηστών. Επίσης κάποια έχουν και διαφορετικές μεθόδους προστασίας.

3. Πρέπει να γράψετε μια αναφορά η οποία περιέχει μια περιγραφή όλων των προσπαθειών τις οποίες εσεις δοκιμάσατε προσπαθώντας να βρείτε μεθόδους εκμετάλευσης των ευπαθών εκτελέσιμων αρχείων. Επίσης η αναφορά σας πρέπει να περιέχει τα μυστικά αρχεία τα οποία ανακαλύψατε. Ακόμη και αν δεν μπορέσατε να βρείτε κάποιο αρχείο πρέπει να γράψετε με λεπτομέρεια όλα τα βήματα τα οποία ακολουθήσατε και να συμπεριλάβετε όλες τις σχετικές πληροφορίες τις οποίες χρησιμοποιήσατε ώστε να δείξετε με αναλυτικό τρόπο την προσπάθεια σας να σπάσετε τους τρεις λογαριασμούς.

Αν καταφέρετε να σπάσετε και τους τρεις λογαριασμούς τότε θα μπορέσετε να βρείτε και ένα τελικό μυστικό το οποίο σχηματίζεται μόνο σε αυτήν την περίπτωση.

Τα υπόλοιπα μπορούν να σας βοηθήσουν στο διάβασμα για την επίλυση του project (ειδικά το πρώτο):

- Smashing the stack for fun and profit, by Aleph One, `http://insecure.org/stf/smashstack.html`. (**ΑΠΑΡΑΙΤΗΤΟ**).
- "Scraps of notes on remote stack overflow exploitation", by pi3, (only up to section 3.1) `http://www.phrack.org/issues.html?issue=67id=13article` (**ΑΠΑΡΑΙΤΗΤΟ**).
- SMASHING C++ VPTRS by rix, PHRACK Volume 0xa Issue 0x38. `http://www.phrack.org/issues.html?issue=56id=8`. (**ΑΠΑΡΑΙΤΗΤΟ**).

- Bypassing non-executable-stack during exploitation using return-to-libc. By c0ntex. `http://css.csail.mit.edu/6.858/2012/readings/return-to-libc.pdf`
- The advanced return-into-lib(c) exploits, PHRACK Volume 0x0b, Issue 0x3a, Phile 0x04 of 0x0e. `http://www.phrack.org/issues.html?issue=58id=4`.
- An introduction to Unix exploits, by Claes M. Nyberg, `http://www.cs.chalmers.se/Cs/Grundutb/Kurser/lbs/usploits.ps`
- PC Assembly, by Paul Carter, `http://www.drpaulcarter.com/pcasm/`
- Stack Smashing Protection for Debian, Debian Administration, `http://www.debian-administration.org/articles/408`

Οδηγίες. Πρέπει να δουλέψετε μόνοι σε αυτό το project. Πρέπει να γράψετε την αναφορά σας ηλεκτρονικά και να την παραδώσετε ηλεκτρονικά στη διεύθυνση : `csec.di@gmail.com` σε μορφή doc, ps η pdf αρχείου. Τα μυστικά αρχεία αλλάζουν συχνά και περιέχουν MAC υπογραφές και χρονολογικά δεδομένα. Αν καταφέρετε να διαβάσετε ένα μυστικό αρχείο μην το μοιραστείτε με τους φίλους σας! Όλα τα αρχεία θα ελεχθούν για ακεραιότα και μοναδικότητα. Μαζί με την αναφορά σας πρέπει να στείλετε στην παραπάνω διεύθυνση και τα μυστικά αρχεία που τυχόν ανακαλύψατε.
Καθυστερημένες Υποβολές Project. Μπορείτε να χρησιμοποίησετε μέχρι 10 μέρες για να καθύστερησετε την παράδωση ενος project (συνολικά για όλο το εξάμηνο). Η ημερομηνία υποβολής κρίνεται η ημερομηνία που παρδίνεται το e-mail σας στον server.
Εξώφυλλο Project. Το εξώφυλλο του project σας πρέπει να περιέχει το όνομα σας, το ΑΜ σας, καθώς και τα στοιχεία ``Project #1", ``ΥΣ13 ΕΑΡΙΝΟ 2014" καθώς και μια ένδειξη για το πόσες μέρες καθυστέρησης χρησιμοποιήθηκαν (`0` αν καμμία).