C/Linux

Projet Noyau: “kernelbrick”

Master III
Julien Hochart – jul@hochart.fr

Introduction

- Noyau (kernel) linux
- Noyau monolithique
- 1991+
- Contrôle de l'OS, interface entre les programmes et le matériel
- Sources sur kernel.org

Introduction

- Vous êtes employé par l'ANSSI, qui vous demande de **livrer un patch secret pour le noyau linux,** répondant à un besoin précis
  - Patch pour kernel vanilla 4.9.162 (4.9 LTS)
  - Un système patché doit avoir le comportement suivant: si un utilisateur lance un programme dont le nom est **code144** , le système devient **immédiatement** inutilisable (processes, shells, réseau, …) et doit être rebooté (mais ne doit pas rebooter tout seul)

Consignes

- Livraison par email avant le **24/04/2019 @ 18h**
  - **RCPT: jul@hochart.fr**
  - **Sujet: Patch NOM**
  - **Attachment: kernelbrick-p.nom-v1.patch**
- Kernel cible: vanilla **4.9.162**
- Patch dans un format normé
- Le kernel patché doit compiler
- Le kernel doit booter et fonctionner normalement
- Le kernel pourra être utilisé avec une distribution quelconque (récente)
- La machine doit rebooter correctement après un hard reset suite à un brick

Consignes

- Fabrication du patch
  - **diff -ruN linux-4.9.162/ linux-4.9.162-new/ > kernelbrick-p.nom-v1.patch**

  - linux-4.9.162 : Répertoire original (vanilla) après décompression de l'archive
  - linux-4.9.162-new: Repertoire après dev de la modification (arborescence propre)

Specs de la correction

- **Application du patch (Sur machine de correction Debian 9.8)**
  - cd && rm -rf builddir && mkdir builddir && cd builddir
  - wget https://cdn.kernel.org/pub/linux/kernel/v4.x/linux-4.9.162.tar.xz && tar xaf linux-4.9.162.tar.xz && echo DONE
  - cp ../rendu/kernelbrick-j.hochart-v1.patch ./current.patch && patch -s -p0 < current.patch && echo PATCH_SUCCESS || echo PATCH_FAIL

Specs de la correction

1. **Build (Sur la machine de correction Debian 9)**
   a. Edition du Makefile pour modifier EXTRAVERSION = -kb-[prenom]-1
   b. make olddefconfig
   c. Build / compilation
   d. Installation du nouveau kernel
   e. Reboot sur nouveau kernel
   f. SSH sur machine de test
   g. cd xxxxx
   h. ./code144

Notation

1. Patch livré dans les temps: **10**
2. Patch apply avec succès (et avec du code dedans): **10**
3. Kernel build après patch non vide: **13**
4. Kernel boot après patch: **14**
5. code144 plante le système: **20**
6. **Soutenance sample en cours (inchangé ou -20)**

7. **Bonus 1:** le système affiche un BSOD sur la console en plantant: **+2**
8. **Bonus 2:** la fonction du patch est raisonnablement incompréhensible pour un relecteur/valideur en 5 minutes: **+2**