SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 30 janvier 2023

Conditions d'examen :

a. Après le tirage au sort d'une enveloppe contenant deux questions traitant de sujets différents, l'examen oral se déroulera en deux phases :
   - une phase de préparation de 20 minutes et
   - une phase de présentation de 20 minutes.

b. Durant la phase de préparation, l'étudiant-e préparera les réponses aux questions sur transparents. Pour sa préparation, l'étudiant-e aura le droit à un résumé de **5 pages imprimées recto-verso sous forme papier**. Les ordinateurs, tablettes ou smartphones ne sont pas autorisés.

c. Durant la phase présentation, l'étudiant-e exposera ses solutions au collège de professeurs au rétroprojecteur et répondra aux questions subsidiaires. Ces questions permettront au collège de professeurs d'établir le niveau de connaissance et de compétences de l'étudiant-e. Durant la présentation, l'étudiant ne pourra utiliser que les transparents rédigés précédemment dans la phase de préparation (ne pourra pas utiliser le résumé).

d. A la fin de l'examen, les questions et les transparents seront récupérés et conservés par le collège de professeurs.

SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 30 janvier 2023

Les étudiant-e-s devront être capable :

Buildroot

1. D'expliquer les principaux répertoires de buildroot
2. D'expliquer le principe de fonctionnement de buildroot
3. D'expliquer la configuration de buildroot pour un hardware donné
4. D'expliquer comment faire un patch et appliquer ce patch dans buildroot
5. D'expliquer comment configurer, compiler buildroot, u-boot, kernel
6. D'expliquer comment la SD-Card est générée
7. D'expliquer comment le rootfs est généré
8. D'expliquer le rootfs_overlay
9. Savoir installer un nouveau package dans buildroot

u-boot

10. D'expliquer le démarrage du NanoPi
11. De connaître, expliquer les principales commandes de u-boot utilisées durant le démarrage
12. De savoir comment configurer u-boot
13. D'expliquer comment améliorer la sécurité de u-boot
14. De connaître les différentes étapes pour la création de l'image de u-boot.itb
15. Savoir ce que fait la commande strip sur un fichier elf
16. De connaître les différentes étapes pour la création de uImage
17. De connaître l'utilité du Flattened Device Tree
18. De connaître de manière générale le mapping de la SDCard
19. D'expliquer le fichier boot.scr

Compilation du noyau

20. De connaître les principaux répertoires du noyau Linux
21. De connaître les principales méthodes pour sécuriser le noyau Linux
22. D'expliquer le principe des software attacks : buffer overflow, ret2libc, ROP
23. D'expliquer le principe des protections contre les softwares attacks : ASLR, PIE, canary

SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 30 janvier 2023

Valgrind

24. De connaître les différents outils de Valgrind et leur utilisation
25. Pour un code donné avec des erreurs, savoir quel-s outil-s de Valgrind utiliser

Hardening Linux

26. De contrôler l'intégrité d'un package, d'un programme
27. De configurer un nouveau package, programme
28. De cross-compiler un programme
29. De contrôler les services, les ports ouverts
30. De contrôler les « file systems »
31. De contrôler les permissions des fichiers, répertoires
32. De sécuriser le réseau
33. De contrôler-sécuriser les comptes utilisateurs
34. De limiter le login root
35. De sécuriser le noyau
36. De sécuriser une application
37. De contrôler le démarrage de Linux
38. D'appliquer la méthodologie OSSTMM simplifiée

Filesystem

39. De connaître les différents types de systèmes de fichiers ainsi que leurs applications
40. De connaître les caractéristiques des filesystems ext2-3-4, ainsi que les commandes associées
41. D'expliquer les différents « files systems » utilisés dans les systèmes embarqués (ext2-3-4, BTRFS, F2FS, NILFS2, XFS, ZFS, …)
42. Expliquer les « files system » de type Journal, B_Tree/CoW, log filesystem
43. De connaître les caractéristiques du filesystem Squashfs, ainsi que les commandes associées
44. De connaître les caractéristiques du filesystem tmpfs, ainsi que les commandes associées
45. De connaître les caractéristiques du filesystem LUKS, ainsi que les commandes associées
46. Savoir expliquer la gestion des clés de LUKS
47. De connaître les caractéristiques du filesystem InitramFS, ainsi que les commandes associées
48. De savoir créer un initramFS

SeS (Secure Embedded System)

Objectifs de l'examen oral du lundi 30 janvier 2023

Filesystems security

49. De connaître les « files permissions » sous Linux
50. De contrôler et sécuriser les comptes utilisateurs sous Linux
51. De connaître les real-effective userID and groupID
52. De connaître les ACL
53. De connaître les attributs particuliers des filesystems ext2-3-4
54. De rechercher des permissions de fichier faibles
55. Comment sécuriser les répertoires temporaires
56. De savoir comment les mots de passe sont mémorisés sous Linux
57. De connaitre les différentes possibilités pour casser un mot de passe
58. De savoir utiliser hashcat pour casser un mot de passe

Firewall Iptables

59. De connaître les principes de Netfilter, iptables
60. Savoir expliquer les notions de chain-tables
61. Savoir expliquer les différences entre les firewall Stateless et Stateful
62. Savoir configurer avec iptables un firewall simple de types Stateless (pages 17-19) et Stateful (pages 26-32)
63. Connaître le principe des NFQUEUE

TPM

64. Savoir expliquer uniquement le principe des chiffrements symétrique, asymétrique, fonctions de hachage, la signature digitale
65. Connaitre les différentes implémentations des TPM (discrete, integrated, Hypervisor, Software)
66. Connaitre l'architecture interne d'un TPM
67. Connaitre les différentes hiérarchies des TPM (endorsement, platform, owner, null)
68. Savoir créer, utiliser des clés avec un TPM
69. Connaitre les commandes principales d'un TPM (pas tous les paramètres, mais savoir expliquer ce que font ces commandes, être capable de dessiner ce que font les commandes)
70. Savoir encrypter-décrypter, signer-vérifier avec un TPM
71. Savoir utiliser les registres PCR
72. Savoir sauver des données sur le TPM
73. Savoir sauver des données et les protéger avec une PCR policy