SEC9 - Sécurité avancée du Linux embarqué

Objectifs

- Apprendre les bases de la sécurité du Linux embarqué
- Comprendre le modèle de menaces de Linux
- Découvrir les fonctions du noyau Linux permettant de durcir la sécurité
- Comprendre les Linux Security Modules
- Apprendre comment le sandboxing peut durcir la sécurité de votre système’s

Prérequis

- Connaissance du langage C (voir par exemple notre formation L2)
- Construction d'une plate-forme Linux embarqué sécurisée (voir par exemple notre formation D11)
- Le cours SEC8 Construction d'une plate-forme Linux embarqué sécurisée peut également vous intéresser
- Le cours SEC1 Développement sécurisé pour systèmes embarqués peut également vous intéresser
- Le cours SEC2 Sécurité avancée des systèmes embarqués peut également vous intéresser

Matériel

- Supports de cours et exercices logiciels
- Un PC Linux pour deux stagiaires
- Une plate-forme cible pour deux stagiaires

Durée

- Total : 3 jours
- De 40% à 50% du temps de formation est consacré aux activités pratiques

Environnement du cours

- Cours théorique
  - Support imprimé et PDF (en anglais).
  - Assistance du formateur tout au long de la formation.
- Chaque session débute par un point avec les stagiaires.

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Plan du cours

Premier jour

Définir le modèle de menaces du Linux embarqué

- Les risques de sécurité potentiels pour un système embarqué
- Modèle de menaces pour le Linux embarqué
  - Identification des actifs et des menaces
  - Comprendre les vecteurs d'attaque
  - Identification des faiblesses de sécurité et des risques

    - Analyse des menaces et évaluation de l'impact
    - Contre-mesures et réduction des menaces
- Réduction de la surface d'attaque
- Vulnérabilités Linux courantes
- Outils Linux vulnérables
- Recherche des vulnérabilités connues

Fonctions de sécurité de base sous Linux

- Gestion des utilisateurs et des groupes
- Permissions et propriété des fichiers
    - Restreindre l'accès aux informations sensibles
    - Limiter l'accès public aux fichiers système
- Ajustement des services système
- Validation des entrées et traitement incorrect des entrées
    - Présentation de la validation des entrées et de son importance
    - Techniques de validation des entrées
    - Prévention et atténuation des attaques liées aux entrées
- Débordement de tampon sur la pile
    - Comprendre l'impact et les techniques d'atténuation
    - Activation des mécanismes de protection de la pile dans le noyau Linux
    - Address Space Layout Randomization (ASLR)
    - Prévenir les attaques sur la pile par la revue de code
- Élévation de privilèges
    - Vecteurs d'attaque par élévation de privilèges
    - Élévation de privilèges horizontale et verticale
    - Exploitation des exécutables SUID
    - Élévation de privilèges via des services mal configurés
    - Élévation multi-utilisateurs
    - Attaques par débordement de tampon
    - Atténuation des attaques par élévation de privilèges
    - Bonnes pratiques pour prévenir l'élévation de privilèges

Durcissement réseau

- Présentation de la sécurité réseau
- Sécurisation de SSH
- Chiffrement du trafic réseau
- Utilisation des certificats SSL/TLS
- Réseau privé virtuel (VPN)
- Sécurité des réseaux sans fil
- Systèmes de détection d'intrusion (IDS) et systèmes de prévention d'intrusion (IPS)
- Pare-feu sous Linux
    - Types de pare-feu disponibles sous Linux
    - Configuration du pare-feu avec iptables, firewalld ou nftables

Deuxième jour

Fonctions de sécurité avancées sous Linux

- Restriction des appels système sous Linux
    - Introduction à la restriction des appels système
    - Comprendre l'objectif et les bénéfices de la restriction des appels système
    - Comment utiliser seccomp pour restreindre les appels système sous Linux
    - Analyse de l'impact des restrictions d'appels système sur le fonctionnement des applications
    - Limitations de seccomp
    - Bonnes pratiques pour établir une liste blanche d'appels système

    - Filtrage des appels système par systemd
- Renforcer la sécurité avec les capabilities
    - Présentation des capabilities sous Linux
    - Comprendre l'importance de la séparation des privilèges sous Linux
    - Les différents types de capabilities
    - Les commandes liées aux capabilities
    - Capabilities du système de fichiers
    - Mise en œuvre des capabilities du système de fichiers
    - Protection des exécutables SUID
    - Renforcement de la sécurité des démons
    - Définition des capabilities par défaut des processus nouvellement créés
    - Études de cas et exemples concrets

Durcissement du noyau Linux

- Méthodes de durcissement du noyau Linux
- Configuration personnalisée du noyau
- Options de durcissement du noyau
- Auto-protection du noyau
- Désactivation des services inutiles
- Limitation des ressources mémoire disponibles

Linux Security Modules (LSMs)

- Introduction aux Linux Security Modules (LSMs)
    - Présentation des LSMs et de leur rôle
    - Types de LSMs disponibles sous Linux
    - Comprendre le modèle de sécurité de Linux
- Permissions d'accès
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)
- Présentation des concepts, objectifs et principes des modèles de sécurité MAC
- Modèles MAC
- Mise en œuvre du MAC
    - listes de contrôle d'accès (ACLs)
    - contrôle d'accès basé sur les rôles (RBAC)
    - contrôle d'accès basé sur les étiquettes (LBAC)
    - Gestion du MAC dans un environnement multi-utilisateurs
    - DAC ou MAC

Security Enhanced Linux (SELinux)

- Présentation de SELinux et de son rôle
- Activation de SELinux
- Architecture et composants
- Contextes et étiquettes SELinux
- Bénéfices de l'utilisation de SELinux
- Politiques SELinux
    - Comprendre les politiques SELinux
    - Création et gestion des politiques SELinux
    - Structure et langage des politiques SELinux
- Modes Enforcing, Permissive et Disabled
- Composants User, Role et Type
- Définition de types de domaine personnalisés
- Valeurs booléennes SELinux
- Audit et journalisation SELinux
- Résolution des problèmes SELinux
- Configuration avancée de SELinux

    - Gestion des contextes de port SELinux
    - Configuration de SELinux pour les services systemd
    - Gestion de SELinux pour les conteneurs

Troisième jour

Autres Linux Security Modules

- AppArmor
    - Présentation des fonctionnalités et possibilités d'AppArmor
    - Mise en œuvre d'AppArmor sous Linux
    - Création et gestion des profils AppArmor
    - Comprendre et utiliser les règles AppArmor
    - AppArmor ou SELinux : choisir la solution adaptée à vos besoins
- Simple Mandatory Access Control for Linux (SMACK)
    - Présentation de SMACK et de son rôle
    - Caractéristiques et fonctionnalités de SMACK
    - Configuration et mise en œuvre de SMACK
    - Personnalisation des politiques SMACK
    - Combinaison de SMACK avec d'autres fonctions de sécurité
    - Forces et faiblesses de SMACK
- TOMOYO
    - Présentation de TOMOYO et de son rôle
    - La différence entre TOMOYO et les autres LSMs
    - Les politiques TOMOYO
- Yama
    - Explication de Yama et de son rôle dans la sécurité de Linux
    - Architecture de Yama et interaction avec les autres LSMs
    - Personnalisation des différentes règles et politiques de Yama
- SafeSetID
    - Importance de SafeSetID pour renforcer la sécurité sous Linux
    - Mise en place des règles et politiques SafeSetID
    - Limitations et difficultés

Validation des modules noyau

- Présentation des composants clés de la signature de modules
- Concepts clés de la signature de modules
- Types de méthodes de signature de modules
    - Discussion des avantages et inconvénients de chaque méthode
- Étapes de la signature d'un module
- Vérification de la signature d'un module chargé
- Prévenir les modules malveillants avec LoadPin
- Étapes d'intégration de LoadPin dans l'environnement Linux

Signature des applications sous Linux

- Signature des paquets pour les gestionnaires de paquets
- Gnu Privacy Guard (GnuPG)
- Integrity Measurement Architecture (IMA)
- The Extended Verification Module (EVM)
- L'outil evmctl

Sandboxing

- Présentation du sandboxing et de son importance
- Comprendre le concept d'isolation et de contrôle des ressources

- Control Groups (cgroups)
- Chroot et ses bénéfices en matière de sécurité
- Conteneurisation avec LXC (Linux Containers)
  - Sécurisation des applications et des démons avec LXC
- Docker et ses fonctions de sécurité
- Exploration des namespaces sous Linux
- Présentation de Firejail

Test, journalisation et audit

- Analyse du système Linux
  - Recherche des logiciels malveillants connus
- Outils d'audit et de surveillance sous Linux
- Examen des journaux à la recherche d'activités suspectes
- Politiques de rétention et archivage des journaux
- Garder les journaux sûrs et protégés contre l'altération ou la suppression