Building a NIDS for a Raspberry Pi in an industrial environment

Type de contenu : Texte

Titre(s) : Building a NIDS for a Raspberry Pi in an industrial environment [texte imprimé] / enseigne de vaisseau Chabert Clément ; enseigne de vaisseau Rudloff Jean-Marie ; organisme d'accueil OSNA research group ; tuteurs de projet Dr. Michael Schukat

Autre(s) auteur(s) : Rudloff, Jean-Marie EN2013

Autre(s) responsabilité(s) : Nui, Galway

Editeur, producteur : Lanvéoc-Poulmic : Ecole navale, 2015

Description matérielle : 1 vol. (IV-50 p.) : ill. en noir et en coul. ; 30 cm

Note de thèses et écrits académiques : PFE Systèmes informatiques et modélisation 2015 Ecole navale

Résumé ou extrait : La protection des systèmes informatiques contre des attaques extérieures est quelque chose de plus en plus nécessaire. L'armée française va dans ce sens en créant un poste consacré à la cyber défense. Notre projet a lui pour but de créer un logiciel pour sécuriser les systèmes industriels. En effet ces derniers sont souvent contrôlés par des systèmes juste assez puissants pour leur fonctionnement, ce qui empêche l'installation de gros programmes de détection faits pour un ordinateur standard. Nous nous sommes tout d'abord intéressés à toute la documentation sur les types de protocoles rencontrés sur une installation industrielle ainsi que les différentes attaques qui en découlent. Ensuite une grosse partie de notre projet a été de créer un logiciel permettant d'être prévenu en cas d'attaques sur le système. Il devait à la fois être efficace et optimisé, pour prendre en compte un grand nombre de données. Nous avons donc produit un système de détection d'intrusion sur les réseaux (NIDS) qui renvoie un message d'erreur pour trois types d'attaques : l'envoi de fausses instructions au système, l'envoi d'un nombre de messages trop élevé et une trop grande demande de connexions au système. Une fois construit, nous avons testé plusieurs outils permettant d'attaquer un système pour mettre à l'épreuve notre programme. Par la suite, le but est de mettre en place un système permettant de récupérer les messages d'alerte provenant des différentes machines sur lesquelles notre NIDS a été installé.