Cryptographie et sécurité
IFT-606

Devoir 2 - Défense

Amandine Fouillet - 14 130 638 & Frank Chassing - 14 153 710

30 mars 2015

Suricata

Le logiciel Suricata est un IPS/IDS open source permettant d'analyser les paquets qui entrent et sortent dans un réseau local afin de donner l'alerte ou bloquer les plus suspects d'entre eux. Au sein de ce logiciel, on retrouve un plugin spécialisé dans l'analyse du contenu des e-mails qui permet de prévenir des attaques d'usurpation d'e-mail. Ce plugin commence par comparer le nom de domaine du destinataire et de l'émetteur. Si ils sont sur le même domaine, l'échange de mail est interne et Suricata doit vérifier que le chemin du mail est conforme. Pour cela, il analyse les serveurs relais par lequel l'e-mail est passé pour aller du point A au point B, si ces serveurs ne sont pas sur la liste blanche définie par l'organisation, le logiciel bloque le mail et alerte l'organisation.

Suricata est performant pour contrer les attaques classiques et habituelles où le hacker s'approprie l'adresse e-mail d'un employé en modifiant seulement le champ FROM du mail. L'efficacité du plugin réside sur le fait que le serveur d'envoi SMTP du hacker est vérifié ainsi que tous les serveurs relais menant au serveur de l'organisation. Le serveur du hacker ne faisant pas partie de la liste blanche, le chemin du mail apparaît frauduleux pour l'IDS et le mail est refusé.

Notre solution pour contourner cette défense consiste à utiliser des serveurs relais présents sur la liste blanche de l'organisation. Habituellement, tous les e-mails envoyés à partir de fournisseurs d'hébergement Web sont approuvés et autorisés. Il suffit donc au hackeur de se connecter à l'un des serveurs mail d'un herbergeur web de confiance et d'envoyer le mail frauduleux à partir de ce serveur. Dans ce cas, Suricata ne sera pas en mesure de discerner l'usurpation car les serveurs relais sont autorisés.