18 Maret 2016

Uswatun Hasanah
18213017

II3230 – KEAMANAN INFORMASI

Topik : **Dionaea - A Malware Capturing Honeypot**

Deskripsi :

Dionaea "Nepenthes penerus" adalah malware penangkap honeypot yang awalnya dikembangkan di bawah The Honeynet Project 2009 Summer of Code (GSoC). Dionaea bertujuan untuk menjebak malware mengeksploitasi kerentanan yang terkena oleh layanan yang ditawarkan melalui jaringan, dan akhirnya mendapatkan salinan dari malware.

Seperti perangkat lunak lain, Dionaea mungkin mengandung bug juga. Dalam rangka meminimalkan dampak, Dionaea berjalan dalam lingkungan yang terbatas tanpa hak administratif.

Dionaea memiliki *modular architecture, embedding Python* sebagai bahasa scripting dalam rangka untuk meniru protokol. Jauh lebih unggul dengan pendahulunya (Nepenthes), ia mampu mendeteksi shellcode menggunakan LibEmu dan mendukung IPv6 dan TLS.

Pada makalah nanti saya akan menjelaskan mengenai latar belakang teknis Dionaea, Setting Up a Dionaea Honeypot dan Dionaea in Action

Referensi:

- http://www.edgis-security.org/honeypot/dionaea/
- Honeypots CERT Exercise Handbook