Techno, ISSN 1410 - 8607
Volume 14 No. 2, Oktober 2013
Hal. 64 – 69

DETEKSI *MALWARE* DALAM JARINGAN MENGGUNAKAN *DIONAEA*

(Malware Detection in the Network Using Dionaea)

Harjono
Program Studi Teknik Informatika, Fakultas Teknik
Universitas Muhammadiyah Purwokerto
Jl.Raya Dukuh Waluh PO BOX 202 Purwokerto 53182
Telp; (0281) 636751 ext 130. Fax. (0281) 637239
email : harjono@ump.ac.id

ABSTRAK

Computer networks connected to the Internet will increase the risk of threats or disruption to the network security. Malware in the form of viruses, worms, and trojan horses is a major threat to the network security. The objective of this research was to detect and identify the malware attacks on the internal network of Muhammadiyah University of Purwokerto using Dionaea. The Dionaea is placed in internal network segmen.A number of attacks to Dionaea originated from several host with private IP addresses from the internal network. Dionaea succesfully download copy of the malware as much as 76 times that consists of only one type of malware that is Win32.Worm.Downadup.Gen. By knowing the type and location of the malware, an appropriate action can be performed.
***Kata kunci** : Malware, Honeypot, Dionaea*

Abstract

Jaringan komputer yang terhubung ke Internet akan memperbesar kemungkinan terjadinya ancaman terhadap keamanan sistem. Malware dalam bentuk virus, worm, dan trojan horses merupakan ancaman utama bagi keamanan sistem jaringan komputer. Penelitian ini bertujuan untuk mendeteksi dan mengidentifikasi serangan malware di dalam jaringan lokal Universitas Muhammadiyah Purwokerto menggunakan Dionaea. Instalasi Dionaea diletakkan pada segmen jaringan internal. Dari penelitian ini didapatkan sejumlah serangan kepada Dionaea yang berasal dari sejumlah host dengan alamat IP private dari dalam jaringan internal. Dionaea berhasil mengunduh salinan malware sebanyak 76 kali yang terdiri dari satu jenis malware saja yaitu Win32.Worm.Downadup.Gen. Dengan diketahuinya jenis dan lokasi malware, maka tindakan yang tepat dapat segera dilakukan.
***Key-words**: Malware, Honeypot, Dionaea*

PENDAHULUAN

Sistem komputer menjadi bagian yang sangat penting dan tidak dapat dipisahkan dalam dunia pendidikan. Jaringan komputer yang terhubung ke internet akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan. *Malicious software* (*malware*) merupakan program komputer yang diciptakan dengan tujuan mencari

kelemahan atau bahkan merusak *software* atau sistem operasi komputer. *Malware* dalam bentuk *virus*, *worm*, dan t*rojan horses* merupakan ancaman utama bagi keamanan sistem jaringan komputer.

Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah terhadap komputer. Sering dijumpai komputer yang program anti virusnya tidak di *update*, atau bahkan tidak dilengkapi dengan program anti virus sama sekali. Hal tersebut menyebabkan komputer atau *host* dapat terinfeksi *malware* tanpa sepengetahuan dari pengguna. Kemudian *malware* tersebut dapat menyebar ke komputer lainnya dalam jaringan, dan pada akhirnya dapat merugikan banyak pihak.

Teknik pengamanan jaringan biasanya dengan memblokade serangan dengan firewall, atau mendeteksi serangan yang ada dengan IDS. Selain menggunakan cara konvensional tersebut, pengamanan sistem jaringan dapat menggunakan *Honeypot* (Kumar, 2009, dan Lopez, 2008). Pada dunia keamanan jaringan, banyak profesional yang sangat tertarik pada *Honeypot* karena seorang pengamat serangan akan dapat melihat informasi secara nyata tentang suatu serangan. Salah satu hal yang bisa didapat dengan *Honeypot* adalah informasi bagaimana seorang penyerang dapat menerobos dan apa yang sudah dilakukannya (Spitzner, 2002).

Dionaea merupakan sebuah *honeypot* yang dirancang untuk menjebak *malware* yang mengeksploitasi kerawanan layanan dalam jaringan, sehingga didapatkan salinan dari *malware* tersebut. *Dionaea* dapat menghasilkan log dalam format basis data menggunakan *SQLite* di samping log dalam format teks, sehingga lebih mudah untuk dilakukan analisis (Suzuki, 2011).

Karena *Dionaea* dapat menentukan *host* yang terinfeksi *malware*, maka tindakan pada *host* yang terinfeksi dapat dilakukan agar dapat dihentikan penyebaran *malware* tersebut ke *host* lain dalam jaringan.

METODE PENELITIAN

Penelitian ini dilakukan di laboratorium jaringan, Teknik Informatika, Fakultas Teknik Universitas Muhammadiyah Purwokerto. Bahan penelitian yang digunakan adalah berupa perangkat lunak yang dipakai untuk menjalankan *Dionaea* di jaringan lokal UMP. Perangkat lunak yang digunakan adalah *Dionaea* yang berjalan di atas sistem operasi *Linux Ubuntu* 10.04. Perangkat lunak pendukung yang digunakan adalah nmap, anti virus BitDefender, online virus *scanner*, gedit, farpd, web browser, dan p0f.

Dalam penelitian ini digunakan alat berupa sebuah perangkat keras komputer dengan spesifikasi yang cukup untuk menjalankan *Honeypot Dionaea* diatas Sistem Operasi *Linux Ubuntu* 10.04. Selain itu juga digunakan perangkat jaringan yang sudah terpasang pada jaringan lokal Universitas Muhammadiyah Purwokerto.

Penelitian diawali dengan melakukan evaluasi jaringan kemudian dilakukan perancangan sistem keamanan yang baru. Pada tahap ini ditentukan lokasi penempatan *Honeypot Dionaea*. Setelah instalasi *Honeypot Dionaea* dan simulasi berhasil seperti yang diharapkan, kemudian *Dionaea* dijalankan.

Dionaea dioperasikan selama satu bulan untuk mendeteksi malware

yang berusaha menyebar di dalam jaringan lokal UMP. Langkah terakhir adalah melakukan analisis terhadap log file yang dihasilkan oleh Dionaea. Analisis ini dilakukan untuk mengetahui berapa banyaknya serangan, sebarapa sering serangan tersebut terjadi, alamat asal serangan, dan jenis *malware* yang menyerang..

HASIL DAN PEMBAHASAN

Dari data yang didapatkan pada tahap evaluasi jaringan, dihasilkan adanya kekurangan atau kelemahan dari keamanan jaringan yang ada yaitu tidak adanya sistem untuk mendeteksi adanya serangan. Untuk meningkatkan keamanan jaringan dibutuhkan sistem yang dapat mendeteksi serta mengidentifikasi ancaman atau serangan, khususnya serangan dari *malware*. Rancangan sistem yang baru dengan menggunakan *Honeypot Dionaea* untuk melakukan deteksi terhadap ancaman atau serangan dari *malware*, yang merupakan ancaman utama bagi keamanan sistem jaringan komputer.

Simulasi terhadap sistem dilakukan untuk mengetahui apakah sistem dapat berjalan sesuai dengan yang diharapkan. *Scanning* terhadap *Dionaea* dilakukan dengan menggunakan software *nmap* terhadap *host* yang menjalankan *Dionaea*. *Scanning* dilakukan baik sebelum maupun setelah Dionaea dijalankan. Hasil scanning dengan nmap sebelum Dionaea dijalankan, seperti ditunjukkan pada Gambar 1. Karena tujuan *Dionaea* adalah untuk menjebak *malware* yang mengeksploitasi kerawanan layanan dalam jaringan, maka layanan yang disediakan oleh *Dionaea* seharusnya terlihat dalam hasil *scanning*. Setelah Dionaea dijalankan kemudian dilakukan pengetesan dengan *nmap* terhadap *host* yang menjalankan *Dionaea* (alamat IP: 10.12.2.122). Hasil *Scanning* menggunakan nmap seperti pada Gambar 2 menunjukkan bahwa *Dionaea* sudah berjalan dengan memberikan layanan yang dapat dijadikan sasaran atau target dari *malware*.

```
File  Edit  View  Terminal  Help
Starting Nmap 5.00 ( http://nmap.org ) at 2011-12-16 15:42 WIT
Interesting ports on 10.12.2.122:
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:21:85:6A:72:72 (Micro-star Int'l Co.)

Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

Gambar 1. Hasil *Scanning* Sebelum *Dionaea* Dijalankan

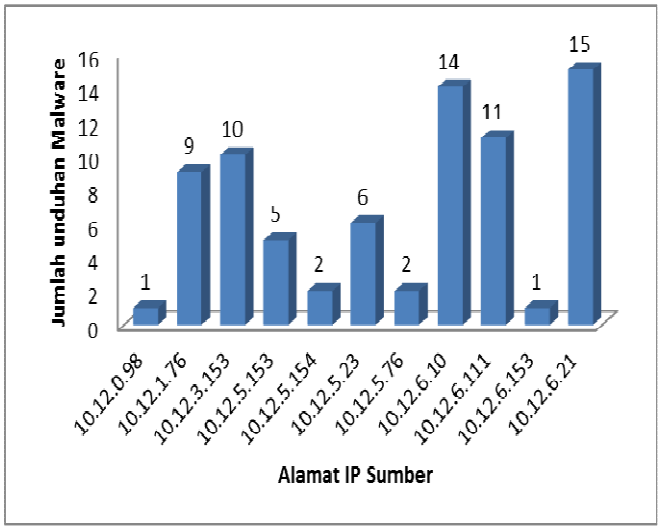
```
File  Edit  View  Terminal  Help
Starting Nmap 5.00 ( http://nmap.org ) at 2011-10-21 15:38 WIT
Interesting ports on 10.12.2.122:
Not shown: 992 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
42/tcp   open  nameserver
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
MAC Address: 00:21:85:6A:72:72 (Micro-star Int'l Co.)

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Gambar 2. Hasil *Scanning* Setelah *Dionaea* Dijalankan

Setelah dilakukan simulasi terhadap *Dionaea*, langkah berikutnya adalah pengujian atau penerapan *Dionaea* dalam jaringan lokal UMP. Pada tahapan ini *Dionaea* dijalankan atau dioperasikan, sehingga dihasilkan data pada file log *Dionaea* jika terdapat aktifitas *malware* yang berusaha menyebar dalam jaringan lokal UMP. Pada penelitian ini *Dionaea* dioperasikan selama satu bulan.

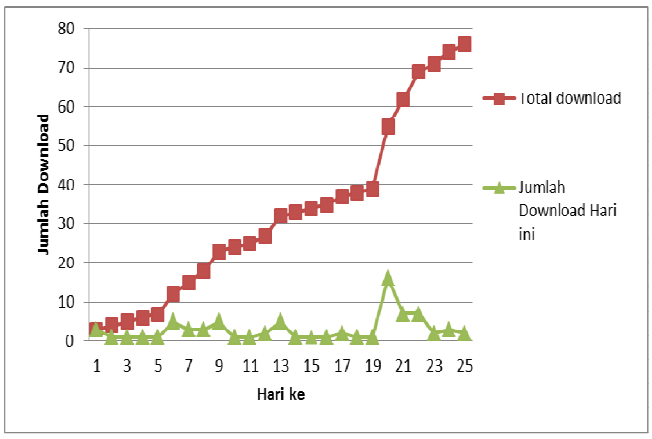
Dari log file yang dihasilkan *Dionaea*, didapatkan data jumlah serangan terbanyak ditujukan kepada port 445 sebesar 89%, kemudian port 80 sebanyak 11%. Port 445 digunakan

oleh windows untuk layanan microsoft-ds. Windows menggunakan TCP port 445 untuk menjalankan protokol SMB (*Server Message Block*) *over* TCP/IP. Protokol SMB merupakan protokol yang digunakan untuk keperluan *sharing*. Sedangkan port 80 adalah layanan http untuk aplikasi web.Terlihat bahwa serangan cenderung mengarah ke port 445. Selama dioperasikan, *Dionaea* berhasil mengunduh *malware* sebanyak 76 kali yang berasal dari sejumlah IP seperti ditunjukkan pada Gambar 3.



Gambar 3. Jumlah Unduhan *Malware* dari Sejumlah IP

Dalam rentang waktu satu bulan jumlah unduhan meningkat secara berangsur-angsur seperti ditunjukkan pada Gambar 4. Rata-rata dalam sehari *Dionaea* mengunduh *malware* sebanyak tiga kali.



Gambar 4. Jumlah Unduhan Malware Setiap Hari

Dari 76 unduhan *malware* tersebut semua mempunyai md5 hash yang sama yaitu: e1855fbe6cf64738bffb9dc195e38ed1. MD5 (*Message-Digest*) adalah fungsi *hash* kriptografi yang menghasilkan nilai *hash* 128-bit (16-byte). MD5 telah digunakan dalam berbagai macam aplikasi keamanan, dan juga biasa digunakan untuk memeriksa integritas data. Untuk dua file yang berbeda tidak akan menghasilkan nilai MD5 *hash* yang sama. Dari hasil tersebut menunjukkan bahwa hanya ada satu jenis *malware* saja. Hasil unduhan dari *malware* tersebut akan tersimpan pada direktori: /opt/dionaea/var/dionaea/binaries/ seperti ditunjukkan pada Gambar 5.

Gambar 5. *Malware* yang Berhasil Diunduh

Untuk mengetahui jenis *malware* yang didapatkan oleh *Dionaea* tersebut digunakan program antivirus. *Malware* yang didapatkan *Dionaea,* oleh antivirus BitDefender dinyatakan sebagai *Win32.Worm.Downadup.Gen*. Selain menggunakan antivirus BitDefender, analisis terhadap *malware* juga dilakukan secara online dengan mengirimkan *malware* tersebut ke virustotal.com, yang akan melakukan analisis *malware* menggunakan 43 program antivirus. Dari 43 program antivirus yang digunakan, 41 dapat mendeteksi *malware* dan hanya dua program antivirus yang tidak bisa mendeteksi *malware* yang didapatkan oleh *Dionaea*. Jadi 95% dari program antivirus yang digunakan oleh virustotal.com dapat mengenali *malware* tersebut. Hampir setiap produk antivirus memberikan nama yang berbeda. Sehingga *malware* yang didapatkan memiliki nama alias yang cukup banyak.

Malware Win32.Worm.Downadup.Gen ini merupakan *worm* yang menginfeksi komputer lain di jaringan dengan memanfaatkan kerentanan dalam layanan Microsoft Windows Server (SVC*HOST*.EXE). Jika kerentanan berhasil dieksploitasi, maka memungkinkan eksekusi *remote code* apabila *file sharing* diaktifkan. *Worm* ini juga dapat menyebar melalui *removable drive* dan *password administrator* yang lemah (Anonymous, 2011).

KESIMPULAN

Dari penelitian ini dapat disimpulkan bahwa serangan yang terdeteksi oleh *Honeypot* berasal dari sejumlah host yang mempunyai alamat *IP private* dari dalam jaringan internal UMP. Hal tersebut menunjukkan bahwa penyerang berasal dari dalam jaringan internal. *Dionaea* berhasil mengunduh *malware* rata-rata tiga kali setiap hari. Jumlah serangan terbanyak ditujukan kepada port 445 sebesar 89%, kemudian port 80 sebanyak 11%. Port 445 digunakan oleh Windows untuk keperluan *sharing,* yang dimanfaatkan oleh *worm* untuk menyebar di dalam jaringan. Serangan yang terdeteksi di jaringan

lokal UMP dilakukan secara otomatis oleh *malware* yaitu *Win32.Worm.Downadup.Gen* yang berusaha menyebar di dalam jaringan.

DAFTAR PUSTAKA

Anonymous, microsoft website, [Online], Available: http://www.microsoft.com/ security/portal/Threat/Encyclopedia /Entry.aspx?name=Worm%3aWin3 2%2fConficker.C, diakses pada tanggal 10 November 2011.

Kumar, S; Pant, D, (2019). *Detection and Prevention of New and Unknown Malware using Honeypots*, International Journal on Computer Science and Engineering Vol.1(2).

Lopez, M. H. Y. dan Resendez, C.F.L. (2008) *Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses*, Proceedings of the Informing Science & IT Education Conference (InSITE).

Spitzner, L. (2002) *Honeypots Tracking Hacker*, Addison Wesley.

Suzuki, H. (2011) Internet Infrastucture Review, Internet Initiative Japan, Vol 11.