

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



SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Jenjang Studi Strata I
pada Program Studi Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh :

Andhik Nugroho

NIM : L200100119

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

2015

LEMBAR PERSETUJUAN

Skripsi dengan judul

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

Yang disusun oleh :

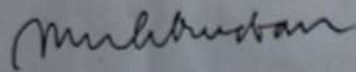
Andhik Nugroho

Telah diperiksa dan disetujui pada :

Hari : Sabtu

Tanggal : 14 Maret 2015

Pembimbing



Muhammad Kushan, S.T., M.T.

NIK :

HALAMAN PENGESAHAN

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

Dipersiapkan dan disusun oleh

ANDHIK NUGROHO

NIM: L200100119

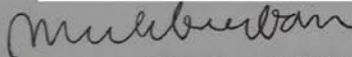
Telah dipertahankan di depan Dewan Penguji

Pada tanggal Juli 2015

Susunan Dewan Penguji

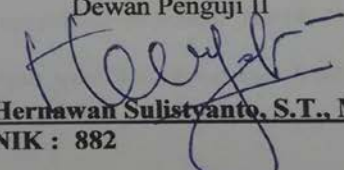
Pembimbing

II


Mohamad Kuslan S.S.T., M.T.
NIK: 663

Husni Tamrin, S.T., M.T., Ph.D.
NIK: 706

Dewan Penguji II


Hernawan Sulistyanto, S.T., M.T
NIK : 882

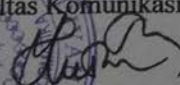
Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 30 Maret 2015

Dekan

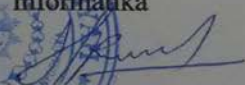
Fakultas Komunikasi dan Informatika


Husni Tamrin, S.T., MT., Ph.D.

NIK : 706

Ketua Program Studi

Informatika


Dr. Heru Supriyono, M.Sc.

NIK : 970

II R O RIRII. I

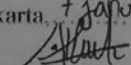
ngan ini saya men atakan bhwa skripsi ini tidak terdapat karya yang pernah diajukan untuk mempemleh g lar kesa janaan eli sualu Per uruan I in i dan sepanjang pngctahuan saya juga tidak terdapat karya atau pendapat yang pernah dituli · atau diterhitkan oleh nran lain kecuali yang seeflrm t rtulis diacu dahtm naskah ini dan disebutkan dalam daftar pustaka.

Beri ut sa.a sampaikan daflar kontribusi dalam penyusunan skripsi ·

1. Penelitian tentang *eksp/oitasi* sistem keamanan *RPC (Remote Procedure Call)* saya lakukan sendiri dan dengan reterensi dari huku , internet dan saat teJadi kesulitan dibantu ternan.
2. Program pendukung yang saya gunakan untuk penelitian ini ialah *Google Chrome 32.0, cmd, Metasp/oit, Free Port Scanner, PrivateFirewal/ 7.0, AVS Firewall don7..oneA/arm Free Firewall.*
3. Saya menggunakan laptop dengan spesi:fikasi *Processor Intel® Core™ i5-240M Proc.eMor 2 20* serta PC dengan pe i:fikasi *Processor Intel Coe to D1111* penelitian ini.

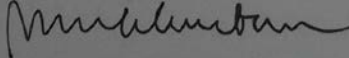
Demikian pernyataan dan daftar kontribusi ini sa a buat dengan ujurnya saya bertanggung jawab atas isi dan kebenaran daftar di atas.

Surakarta, 7 Januari2015


Andhik Nugroho

Mengetahui,

Pembimbing,



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

NIK : 663

MOTTO DAN PERSEMBAHAN

MOTTO :

“Mimpi adalah kunci untuk kita menaklukkan dunia“

(Nidji “Laskar Pelangi”)

“Jangan membuat keputusan ketika sedang MARAH dan jangan membuat janji
sewaktu sedang GEMBIRA“

(Saidina Ali Bin Abi Talib)

”Berusahalah sampai batas akhirmu, agar kau tahu sejauh mana batas kemampuan
yang ada pada dirimu”

(Penulis)

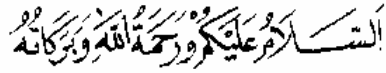
PERSEMBAHAN :

Sebagai rasa syukur dan terima kasih saya persembahkan karyaku ini kepada :

1. Ibu dan Bapak tercinta, tersayang Ibu Sri Sudami dan Bapak Anggono Sari yang senantiasa memberikan doa, dukungan, dorongan, perhatian yang tiada henti-hentinya selama pembuatan karya megah bagi penulis dan dapat membanggakannya.
2. Keluarga tercinta yang selalu mendoakan menghibur, memberikan dorongan, mendukung, menasehati dan memotivasi agar selalu semangat hingga skripsi selesai dan lulus seperti yang di harapkan.
3. Kakak tercinta mbak Titin Sri Hapsari dan mas Dana Ari Sandi, yang sudah mendoakan, membantu penulis dalam menyelesaikan kuliah.

4. Keponakan dan sepupu tercinta Faatih, Fahri, Riska yang sudah menemani dan selalu bikin rame dalam pengerjaan skripsi.
5. Pambudi, Damar, Heri, dan Taufik yang selalu mau diajak refreshing ketika penulis sudah jenuh berada didepan layar Laptop.
6. Teman-teman BBMan yang selalu bikin rame smartphone penulis.
7. Biro skripsi Mas Fauzan dan Aji Saputra yang membantu saya dan memberi semangat dan motivasi.
8. Teman-teman yang selalu membuat rame dikampus Benny, Mul, dan Abdan.
9. Teman TI seangkatan 2010 khususnya kelas D Ahmad, Andrean, Candra, Dodhy, Fenny, Fahrudin Al Ansori (komo), Galih, Hasan, I'in, Lilis, Lutvi cewek, Lutvi cowok, Mukhrom, Novita, Pahrudin, Mak Hanung, Tri Budiyanta (josua), Aulia madina (uli), David, Wahyu Andri.
10. Terima kasih kepada mbak sayang yang selalu memberikan semangat.
11. Terima kasih kepada Mas Sapto yang telah membantu dan memberikan saran pengerjaan skripsi kepada penulis.
12. Teman TI seangkatan.
13. Semua pihak yang telah membantu serta mendoakanku untuk kelancaran skripsi ini yang tak dapat disebutkan satu persatu.

KATA PENGANTAR



Alhamdulillah, puji syukur penulis panjatkan kehadiran Allah SWT yang telah melimpahkan rahmat taufik hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini. Shalawat serta salam semoga tetap tercurah kepada junjungan Nabi Muhammad SAW beserta keluarga, sahabat dan para tabi'in yang telah menyampaikan risalah sehingga umat ini terlepas dari belenggu kesesatan yang berlarut-larut.

Skripsi ini disusun untuk memenuhi kurikulum pada Program Studi Informatika Universitas Muhammadiyah Surakarta, sebagai kewajiban mahasiswa dalam rangka menyelesaikan program sarjana. Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh karena itu kritik saran yang membangun dari berbagai pihak sangat penulis harapkan demi perbaikan-perbaikan ke depan.

Penyelesaian tugas akhir skripsi ini tentunya tidak lupa atas bantuan dari berbagai pihak, oleh karena itu, dengan tulus ikhlas dan kerendahan hati penulis mengucapkan rasa terima kasih sebesar-besarnya kepada :

1. Allah SWT atas segala nikmat, petunjuk, kemudahan, kelancaraan serta kebarokahan sehingga penulis bisa menyelesaikan tugas akhir skripsi ini.
2. Kedua orangtua, Nenek, Kakak, dan keluarga tercinta yang selalu memberikan doa, semangat, nasehat, perhatian yang tak putus-putus sehingga penulis bisa lulus dan semoga dapat membuat bangga mereka.
3. Bapak Husni Thamrin, S.T, MT., Ph.D. selaku Dekan Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.

4. Bapak Dr. Heru Supriyono, S.T., M.Sc. selaku Ketua Jurusan Teknik Informatika Universitas Muhammadiyah Surakarta.
5. Bapak Muhammad Kusban, S.T.,M.T. pembimbing skripsi Penulis yang telah memberikan bimbingan dan pengarahan kepada penulis sehingga dapat menyelesaikan tugas akhir ini.
6. Segenap dosen dan karyawan prodi Teknik Informatika atas bantuan dan ilmu yang diberikan kepada penulis selama masa perkuliahan hingga dinyatakan mendapat gelar Strata 1.
7. Semua pihak yang tidak bisa disebutkan satu-persatu yang telah membantu hingga terselesainya skripsi ini.

Akhirnya penulis berharap semoga skripsi ini berguna bagi semua pihak dan bermanfaat bagi penulis khususnya dan pembaca pada umumnya dalam menambah pengetahuan dan wawasan ilmu. Amiin.

وَالسَّلَامُ عَلَيْكُمْ وَرَحْمَةُ اللَّهِ وَبَرَكَاتُهُ

Surakarta, 7 Januari 2015



Penulis

DAFTAR ISI

Halaman Judul.....	i
Halaman Persetujuan.....	ii
Halaman Pengesahan.....	iii
Daftar Kontribusi.....	iv
Motto dan Persembahan.....	v
Kata Pengantar.....	vii
Daftar Isi.....	ix
Daftar Tabel.....	xii
Daftar Gambar.....	xiii
Abstraksi.....	xv
BAB I PENDAHULUAN.....	1
Latar Belakang Masalah.....	1
Rumusan Masalah.....	2
Batasan Masalah.....	2
Tujuan Penelitian.....	3
Manfaat Penelitian.....	3
Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	6
Telaah Penelitian.....	6
Landasan Teori.....	8
RPC (Remote Procedure Call).....	8
LAN.....	9

2.2.3	Client dan Server	10
2.2.4	Metasploit	10
2.2.5	Free Port Scanner	11
2.2.6	Windows Server 2008	11
2.2.7	Keamanan Jaringan	11
2.2.8	PrivateFirewall 7.0	16
2.2.9	AVS Firewall	17
2.2.10	ZoneAlarm Free Firewall.....	18
BAB III METODE PENELITIAN		19
3.1.	Waktu dan Tempat Penelitian.....	19
	Peralatan Utama dan Pendukung	19
	Peralatan Utama.....	19
3.2.1	Peralatan Pendukung.....	20
	Alur Penelitian.....	20
	Metodologi Penelitian	23
	Langkah Penelitian.....	24
	Implementasi Eksploitasi RPC.....	25
	Deteksi Sistem.....	26
BAB IV HASIL DAN PEMBAHASAN		28
	Hasil Penelitian.....	28
	Setting IP dan Ping.....	28
	Percobaan Eksploitasi pengcopyan File.....	30
	Percobaan Eksploitasi Penggantian Password Administrator.....	40

Percobaan Eksploitasi Reboot.....	41
Defending Menggunakan PrivateFirewall 7.0	42
Defending Menggunakan AVS Firewall.....	47
Defending Menggunakan ZoneAlarm Free Firewall.....	51
Perbandingan diantara Ketiga Firewall.....	55
Hasil Penelitian.....	56
BAB V PENUTUP	61
Kesimpulan.....	61
Saran.....	62
DAFTAR PUSTAKA	63
LAMPIRAN	

DAFTAR TABEL

Tabel 4.1: Daftar Perbandingan Firewall.....	55
Tabel 4.2: Hasil Percobaan Eksploitasi.....	57

DAFTAR GAMBAR

Gambar 2.1 : Prinsip Dasar RPC	9
Gambar 2.2 : Jaringan Client-Server.....	10
Gambar 2.3 : Keamanan Jaringan	16
Gambar 3.1 : Flowchart system alur Penelitian	21
Gambar 3.2 : Scanning Port	26
Gambar 4.1 : Pengaturan IP Address	29
Gambar 4.2 : Ping terhadap IP Target Melalui CMD	30
Gambar 4.3 : Tampilan Awal pada Aplikasi Metasploit.....	31
Gambar 4.4 : Scanning IP yang Aktif dengan Nmap	31
Gambar 4.5 : Macam-macam Perintah pada Metasploit	32
Gambar 4.6 : Penggunaan Perintah Metasploit untuk Eksploitasi	32
Gambar 4.7 : Tampilan Perintah Show Options Pada Aplikasi Metasploit.....	33
Gambar 4.8 : Tampilan Perintah Set RHOST pada Metasploit	33
Gambar 4.9 : Tampilan Perintah set LHOST pada Metasploit	34
Gambar 4.10 : Tampilan Perintah set Payload pada Metasploit	34
Gambar 4.11 :Indikasi Eksploitasi berhasil dengan adanya Perintah Meterpreter	35
Gambar 4.12 : Mengetikkan Perintah Shell dan Masuk ke System Komputer Target..	36
Gambar 4.13 : Drive Z / hack yang masih kosong untuk penyimpanan hasil copyan ...	37
Gambar 4.14 : Mapping Drive F ke Drive Z untuk melakukan Pengcopyan	38
Gambar 4.15 : Langkah Pengcoyan File pada Komputer Target.....	38

Gambar 4.16 : Hasil Pengcopyan file dari Komputer Target	39
Gambar 4.17 : Menutup Drive Z	39
Gambar 4.18 :Tampilan Perintah Hashdump pada Metaspolit	40
Gambar 4.19 : Tampilan Penggantian Password pada Jendela Metasploit	41
Gambar 4.20 : Tampilan dari Proses Reboot pada Jendela Metasploit	41
Gambar 4.21 : Tampilan Desktop PrivateFirewall	42
Gambar 4.22 : Isi Jendela Applications dari Menu PrivateFirewall	43
Gambar 4.23 : Tampilan Jendela PrivateFirewall Log	45
Gambar 4.24 : Tampilan Jendela Port Tracking	46
Gambar 4.25 : Tampilan PrivateFirewall Alert	47
Gambar 4.26 : Tampilan Desktop AVS Firewall	48
Gambar 4.27 : Tampilan Menu Statistics pada AVS Firewall	50
Gambar 4.28 : Tampilan AVS Firewall Alert	51
Gambar 4.29 : Tampilan Desktop ZoneAlarm Free Firewall	52
Gambar 4.30 : Tampilan Menu Tools pada ZoneAlarm Free Firewall	53
Gambar 4.31 : Tampilan Log Viewer	54

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*. *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, Eksploitasi, Client-Server, TCP