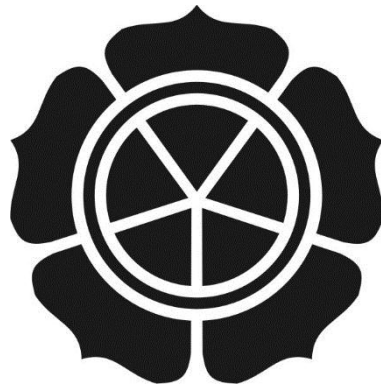


**EXPLOIT DEVELOPMENT MENGGUNAKAN BAHASA
PEMOGRAMAN ASSEMBLY DAN PYTHON UNTUK
MENGAUDIT KEAMANAN PADA
UBUNTU SERVER 64 BIT**

SKRIPSI



disusun oleh :

Muhammad Pailus

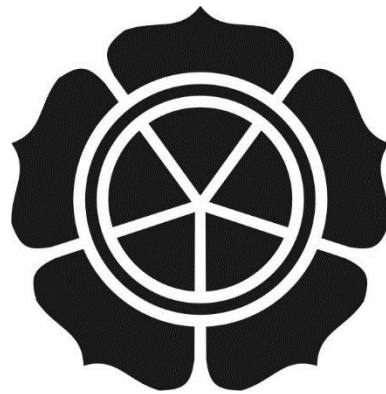
12.11.6109

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

**EXPLOIT DEVELOPMENT MENGGUNAKAN BAHASA
PEMOGRAMAN ASSEMBLY DAN PYTHON UNTUK
MENGAUDIT KEAMANAN PADA
UBUNTU SERVER 64 BIT
SKRIPSI**

Untuk memenuhi sebagian persyaratan
mencapai derajat sarjana s1

Pada Jurusan Teknik Infomatika



disusun oleh

Muhammad Pailus

12.11.6109

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

PERSETUJUAN

SKRIPSI

**EXPLOIT DEVELOPMENT MENGGUNAKAN BAHASA
PEMOGRAMAN ASSEMBLY DAN PYTHON UNTUK
MENGAUDIT KEAMANAN PADA
UBUNTU SERVER 64 BIT**

yang disusun oleh

Muhammad Pailus

12.11.6109

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Nopember 2015

Dosen Pembimbing,



Emha Taufiq Lutfhi, M.Kom

NIK. 190302125

PENGESAHAN

SKRIPSI

**EXPLOIT DEVELOPMENT MENGGUNAKAN BAHASA
PEMROGRAMAN ASSEMBLY DAN PYTHON UNTUK
MENGAUDIT KEAMANAN PADA
UBUNTU SERVER 64 BIT**

yang disusun oleh

Muhammad Pailus

12.11.6109

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 November 2015

Susunan Dewan Penguji

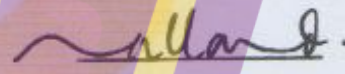
Nama Penguji

Yuli Astuti, M.Kom
NIK. 190302146

Akhmad Dahlan, M.Kom
NIK. 190302174

Emha Taufiq Lutfhi, M.Kom
NIK. 190302125

Tanda Tangan



Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 November 2015

KETUA STMIK AMIKOM YOGYAKARTA



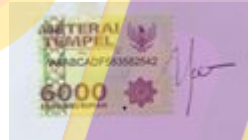
Prof. Dr. M. Suvanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 12 Oktober 2015



Muhammad Pailus

NIM. 12.11.6109

MOTTO



PERSEMBAHAN

Segala bentuk perjuangan selama hampir 4 tahun menuntut ilmu di kampus tercinta ini, dan hasil karya yang menyatakan penulis lulus salah satunya adalah lembar skripsi ini. Semoga semua yang ada dalam karya ini bisa memberikan manfaat bagi siapa saja yang membacanya berikut terimakasih dari penulis terhadap orang-orang yang telah berjasa dalam kehidupan penulis maupun pembuatan skripsi ini.

Untuk Ibu Dan Ayah Tercinta: Tentunya tidak ada karya ini bahkan kehidupan penulis jika tanpa jasa mereka berdua Ibu (Salbiana) dan Ayah (Anasri), rasa terimakasih yang tiada terhingga walaupun penulis menyadari sebanyak apapun penulis mengucapkan terimakasih tidak akan bisa membalas jasa-jasa mereka. Tetapi setidaknya karya berupa skripsi ini bisa memberikan senyuman di wajah mereka yang tentunya penulis sayangi dengan segenap jiwa.

Untuk Kakak Hajri Naito: kehidupan yang membuat penulis harus bekerja sambil kuliah membuat hampir lupa dengan tanggung jawab kuliah untuk menyelesaikan karya ini. Kakak yang memberikan semangat untuk mengutamakan skripsi ini terlebih dahulu untuk di selesaikan. Terimakasih kak untuk semuanya.

Untuk Adek Nopri Ramadhan: sebagai seorang kakak penulis juga merasa perlu memberikan ucapan terimakasih kepada adik semata wayang penulis yang tentunya selalu tersirat doa' untuknya. Nopri yang sekarang sedang menempuh

pendidikan agama semoga menjadi anak yang soleh yang mampu memberikan manfaat untuk umat dan kedua orang tua penulis .

Untuk Rekan Kerja(Danang, Kurniawan): sebagai rekan kerja banyak sekali ilmu yang bisa penulis dapatkan untuk mendalami dunia computer terutama security sesuai dengan bidang yang penulis tekuni. Terimakasih atas ilmu dan kerja samanya selama ini sehingga penulis bisa memasukan beberapa referensi tambahan dari mereka berdua.



DAFTAR ISI

JUDUL	i
PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN	v
Motto	vi
PERSEMBAHAN	vii
DAFTAR ISI	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
ABSTRACT	xvi
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan masalah	2
1.3 Batasan Masalah	3
1.4 Maksud dan Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Metode penelitian	4
1.7 Sistematika Penulisan	4
BAB II	6
LANDASAN TEORI	6
2.1 Tinjauan Pustaka	6
2.2 Exploit Development	7

2.2.1 Exploit.....	7
2.2.2 Payload.....	8
2.2.3 Vulnerability	8
2.2.4 Metasploit Framework.....	9
2.3 Server.....	10
2.4 Audit	11
2.5 Bahasa Pemograman	11
2.6 Bahasa Pemrograman Assembly	11
2.7 Python.....	13
2.8 Keamanan Komputer.....	14
2.9.1 Ping of Death	16
2.9.2 Denial of Service	16
2.9.3 Syn Flood.....	17
2.9.4 Brute Force	17
2.9.5 UDP Flood	18
2.10 Ubuntu server	18
2.11 GDB Debugger	18
2.12 Nasm.....	19
2.13 Reverse Engineering.....	21
2.14 Buffer Overflow	23
2.14.1 Heap Corruptions	24
2.14.2 Stack Overflow	24
2.15 Processor Register	24
2.15.1 Indexing Register	26
2.15.2 Stack Register	26

2.15.3 RIP Register	27
2.16 Reconnaissance	27
2.17 Scanning	28
2.17.1 Fuzz testing.....	29
2.17.2 Port Scanning.....	31
2.18 Eksploitasi.....	32
BAB III	38
METODE PENELITIAN	38
3.1 Gambaran Umum Ruang Fokus Media.....	38
3.1.1 Visi	39
3.1.2 Misi	39
3.1.3 Struktur Organisasi	39
3.2 Alat dan Bahan	40
3.2.1 Kebutuhan Software	40
3.2.2 Kebutuhan Hardware	41
3.2.3 Kebutuhan Fungsional	41
3.3 Kerangka berpikir	42
3.4 Alur Penelitian	44
3.4.1 Identifikasi.....	44
3.4.2 Eksploitasi	44
3.4.2 Covering Track	45
3.4.3 Mitigasi	46
BAB IV	47
HASIL DAN PEMBAHASAN.....	47
4.1 Proses Pengujian dan Exploit Development.	47

4.2 Skenario Pengujian.....	47
4.3 Proses Identifikasi	47
4.3.1 Scanning Menggunakan Nmap.....	48
4.4 Eksploitasi.....	51
4.4.1 Informasi POC dan membuat Code Program	52
CVE-2015-3306 (exec Cmd).....	52
4.4.2 Proses Porting Meterpreter Script.....	57
4.4.3 Membuat shellcode	58
4.4.4 Menggunakan Metasploit (Msfconsole).....	59
4.5 Membuat shellcode Dengan Assembly 64 bit.....	69
4.5.1 Instalasi Dan Konfigurasi	70
4.5.2 Memulai Assembly	71
4.6 Covering Track.....	75
4.6.1 Proses Pengecekan.....	75
4.6.2 Proses Pembersihan	76
4.7 Mitigasi.....	77
BAB V.....	78
PENUTUP.....	78
5.1 Kesimpulan.....	78
5.2 Saran	79
DAFTAR PUSTAKA	80
LAMPIRAN	

DAFTAR TABEL

Tabel 2.1 Perbandingan.....	7
Tabel 2. 2 Register Prosesor.....	26
Tabel 4. 1 Hasil scanning mode Stealth.....	49
Tabel 4. 2 Informasi CVE dari aplikasi yang berjalan	52
Tabel 4. 4 Cara menjalan program untuk melakukan eksploitasi.....	54
Tabel 4. 5 Hasil capture dari wireshark.....	55
Tabel 4. 6 Program melakukan pengiriman perintah.....	56



DAFTAR GAMBAR

Gambar 2. 1 Tampilan Metasploit Framework Mode text.....	10
Gambar 2. 2 Instruksi Bahasa Assembly.....	13
Gambar 2. 3 Gambar Python Dengan mode Interpreter	14
Gambar 2. 4 Grafik penyerangan yang terjadi pada tahun 2014	15
Gambar 2. 5 Simulasi penyerangan DDOS secara real time	17
Gambar 2. 6 Nasm pada terminal Linux 2.11 Bash shell.....	20
Gambar 2. 7 Bash Shell pada linux.....	21
Gambar 2. 8 Fuzz Testing Phase	30
Gambar 2. 9 Remote Scanning	32
Gambar 2. 10 ASLR.....	35
Gambar 2. 11 Stack register 64 bit.....	37
Gambar 3. 1 Struktur Organisasi.....	40
Gambar 3. 2 Proses Penelitian	43
Gambar 3. 3 Proses Exploit Development	43
Gambar 4. 1 Scanning dengan nmap.....	48
Gambar 4. 2 Hasil Scanning dengan version mode	50
Gambar 4. 3 Port Scanning Validation.....	51
Gambar 4. 4 Bagian Code untuk eksploitasi proftpd 1.3.5.....	53
Gambar 4. 5 Cara menjalankan program untuk melakukan eksploitasi	54
Gambar 4. 6 Hasil capture dari wireshark.....	55
Gambar 4. 7 Program melakukan pengiriman perintah	56
Gambar 4. 8 Porting dari python ke meterpreter scripting.....	57
Gambar 4. 9 proses generate shellcode	58
Gambar 4. 10 menjalankan service postgresql.....	59
Gambar 4. 11 menjalankan service metasploit.....	60
Gambar 4. 12 msfconsole dengan mode text	60
Gambar 4. 13 Proses Pencarian tipe exploit.....	61
Gambar 4. 14 informasi yang diperlukan oleh program	62

Gambar 4. 15 Proses mengisi informasi target	62
Gambar 4. 16 payloads yang tersedia	63
Gambar 4. 17 Berhasil mengambil alih shell dengan reverse python.....	64
Gambar 4. 18 proses mendownload admin.php (php shell).....	65
Gambar 4. 19 Proses membuat server handler.....	65
Gambar 4. 20 Mengisi requiremen.	66
Gambar 4. 21 Mengisikan informasi payload	67
Gambar 4. 22 Server handler sudah berada dalam posisi listen.....	67
Gambar 4. 23 menjalankan shell yang berada pada server	68
Gambar 4. 24 Server handler telah berhasil mengambil alih target.....	69
Gambar 4. 25 Pilihan perintah Meterpreter.....	69
Gambar 4. 26 instalasi program nasm dan build essential	70
Gambar 4. 27 Gambar memula assembly shellcode	71
Gambar 4. 28 Cara mencari numerik Library untuk TCP.....	72
Gambar 4. 29 Open Port 444 untuk listen.....	72
Gambar 4. 30 Gambar Potongan kode program Execve shell	73
Gambar 4. 31 Gambar Proses Compiler dan linker assembly	74
Gambar 4. 32 Gambar testing berhasil.....	74
Gambar 4. 33 Hasil scan setelah di lakukan pengujian.....	75
Gambar 4. 34 Sisa hasil shellcode yang di upload.....	76

ABSTRACT

Assembly language is a low-level programming language, assembly language is the one language that can interact directly with the processor. Assembly language besides one of the languages used to build the operating system, especially for communication with the hardware. In assembly language application can be utilized to perform application or system audit operating system. Because assembly language is a low-level language that can be utilized to manipulate the working of processor registers.

Python is one of the high-level programming language, usually applied to programming desktop, web, and on. However here python will be combined with the assembly to facilitate its application. Linux server operating system is one of the most widely used for servers in the world. When this increased server utilization will also directly proportional to the vulnerabilities that arise, as a result of the development of human knowledge also in the field of Computer. To minimize the threat of a server from the attacker, it is necessary to the security audit. One method for security auditing is using Exploit Development. Exploit development is a method to find a gap an operating system or application using assembly language combined with a python.

Keyword : Exploit Development, Assembly, Python, Vulnerabilities