

**TESTING PENETRASI PADA SERVER PROXY WARNET
GALERI INFORMATIKA KECAMATAN SEMIN
KABUPATEN GUNUNGKIDUL**

SKRIPSI



disusun oleh

Adam Ghifari Nuskara

09.11.2670

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

TESTING PENETRASI PADA SERVER PROXY WARNET

GALERI INFORMATIKA KECAMATAN SEMIN

KABUPATEN GUNUNGKIDUL

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Adam Ghifari Nuskara

09.11.2670

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

PERSETUJUAN

SKRIPSI

**TESTING PENETRASI SERVER PROXY PADA WARNET
GALERI INFORMATIKA KECAMATAN SEMIN
KABUPATEN GUNUNGKIDUL**

yang dipersiapkan dan disusun oleh

Adam Ghifari Nuskara

09.11.2670

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 4 Juni 2014

Dosen Pembimbing



Melwin Syafrizal, S.Kom, M. Eng.
NIK. 190302105

PENGESAHAN

SKRIPSI

**TESTING PENETRASI SERVER PROXY PADA WARNET
GALERI INFORMATIKA KECAMATAN SEMIN
KABUPATEN GUNUGKIDUL**

yang dipersiapkan dan disusun oleh

Adam Ghifari Nuskara

09.11.2670

telah dipertahankan di depan Dewan Penguji
pada tanggal 3 Juni 2014

Susunan Dewan Penguji

Nama Penguji

Mei P. Kurniawan, M.Kom
NIK. 190302187

Barka Satya M.Kom
NIK. 190302126

Melwin Syafrizal, S.Kom, M.Eng.
NIK. 190302105

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 4 Juni 2014


KETUA STMHK AMIKOM YOGYAKARTA



Prof. Dr. M. Suyanto, MM.
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, 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.



Yogyakarta, 4 Juni 2014

Adam Ghifari Nuskara
09.11.2670

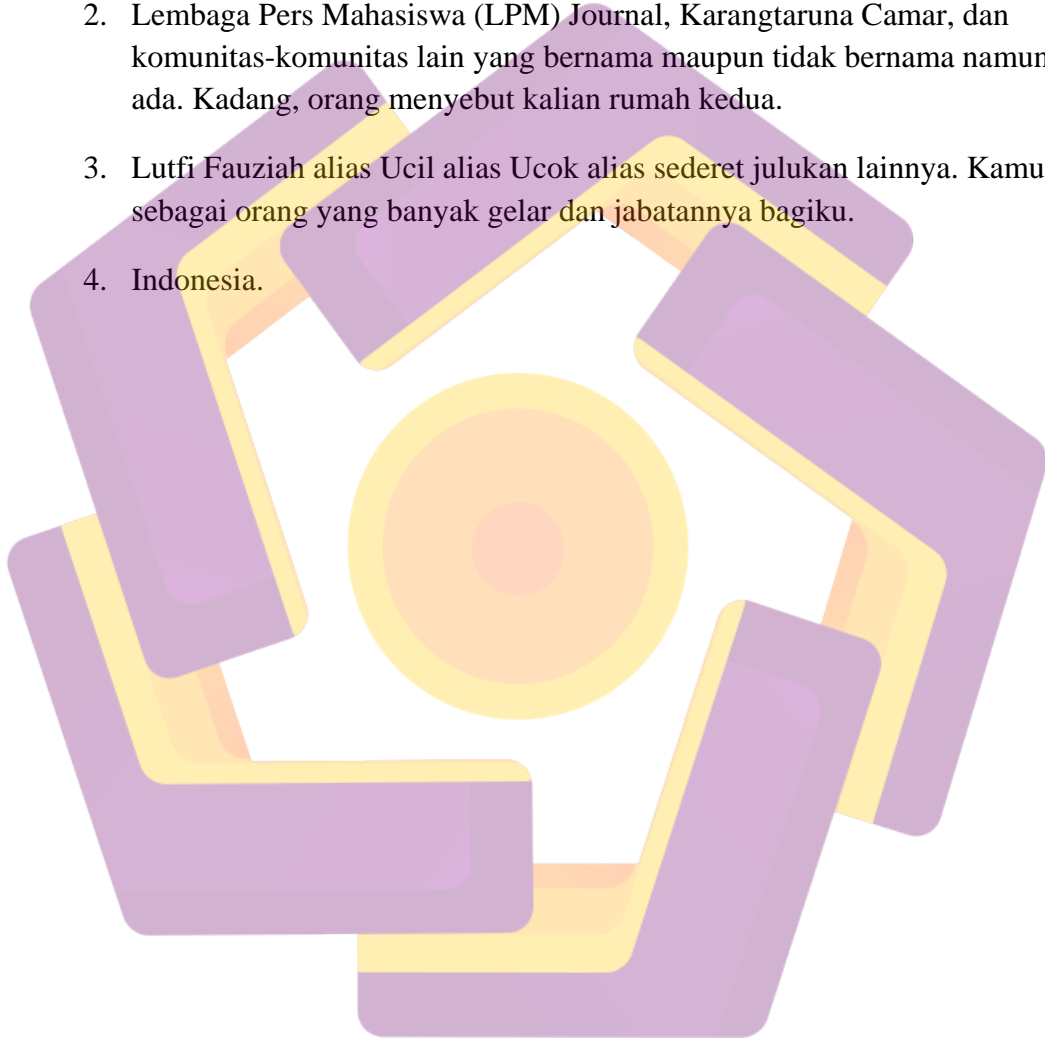
MOTTO

Aku sering berganti-ganti motto. Semauku sendiri. Maka yang paling penting adalah ikuti saja kata hatimu.



PERSEMBAHAN

1. Mama dan Papa selaku pemberi beasiswa paling lama, Rere sebagai pemilik Lenovo G480, Della sebagai tempat mencurahkan segala kenakalan dan kejahilanku.
2. Lembaga Pers Mahasiswa (LPM) Journal, Karangtaruna Camar, dan komunitas-komunitas lain yang bernama maupun tidak bernama namun ada. Kadang, orang menyebut kalian rumah kedua.
3. Lutfi Fauziah alias Ucil alias Ucok alias sederet julukan lainnya. Kamu sebagai orang yang banyak gelar dan jabatannya bagiku.
4. Indonesia.



KATA PENGANTAR

Puji syukur kepada Allah SWT. yang telah memberikan petunjuk, hidayah, kesehatan, dan rezeki sehingga penulis dapat menyelesaikan tugas akademik.

Skripsi ini diharapkan dapat berguna bagi obyek penelitian; Warnet Galeri Informatika, sebagai alat ukur konsep keamanan jaringan yang diterapkan. Rekomendasi yang penulis sampaikan, semoga dapat menyempurnakan.

Kekurangan masih dapat ditemukan dalam penyusunan skripsi ini. Maka penulis menerima kritik dan saran yang membangun agar menjadi upaya memperbaiki diri bagi penulis. Selibhnya, penulis menyampaikan permohonan maaf apabila terdapat kesalahan.

Dengan ini penulis menyampaikan ucapan terimakasih kepada:

1. Kedua orang tua, atas segala perjuangan yang lebih keras untuk membantu penulis berjuang menyelesaikan skripsi.
2. Bapak Melwin Syafrizal, S.Kom, M.Eng atas bimbingan, kritik, dan saran kepada penulis dari awal hingga akhir penyusunan skripsi ini.
3. Bapak Rudy Rakhmadi, MCP, MCSE, MCDDBA, ENSA, CEH, ECSP atas *share* ilmu dan materinya.
4. Bapak Mujoko beserta Saudara Pondra Janu Arga Dewangga dari Warnet Galeri Informatika, atas izin penelitian di lokasi.
5. Semua pihak yang turut membantu penyusunan skripsi ini dari awal hingga akhir.

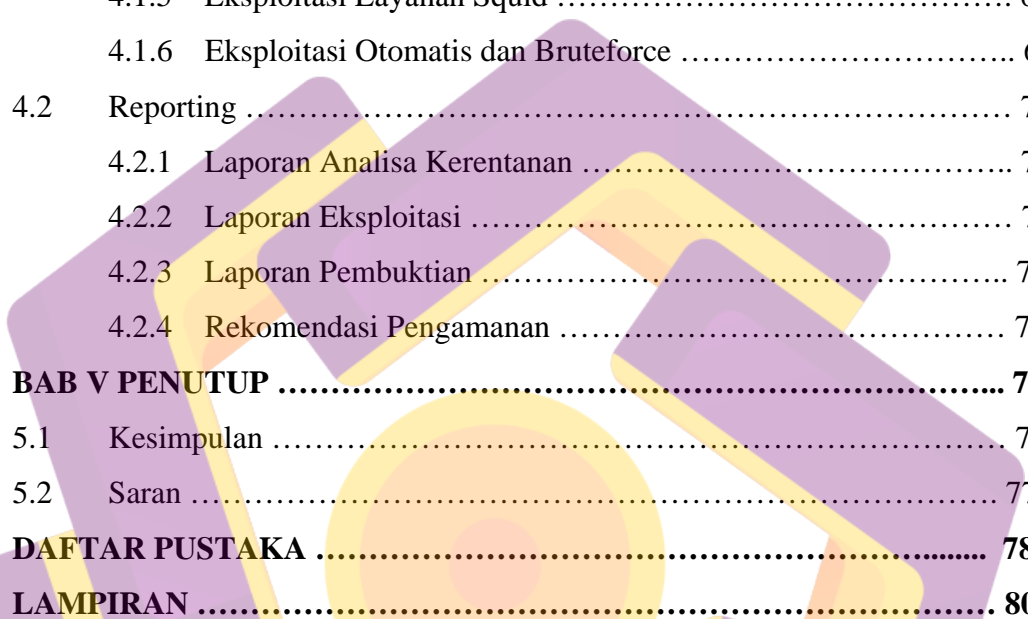
Yogyakarta, 4 Juni 2014

Penulis

DAFTAR ISI

JUDUL.....	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
BAB I Pendahuluan	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian	4
1.7 Sistematika Penulisan	5
1.8 Rencana Kegiatan	6
BAB II Landasan Teori	6
2.1 Tinjauan Pustaka	7
2.2 Penetration Testing	8
2.2.1 Definisi Penetration Testing	8
2.2.2 Legalitas Penetration Testing	9
2.2.3 Mekanisme Penetration Testing	10
2.2.4 Tools Penetration Testing	12
2.3 Proxy	14
2.3.1 Definisi Server Proxy	14
2.3.2 Squid	16
2.4 Serangan Terhadap Jaringan	16

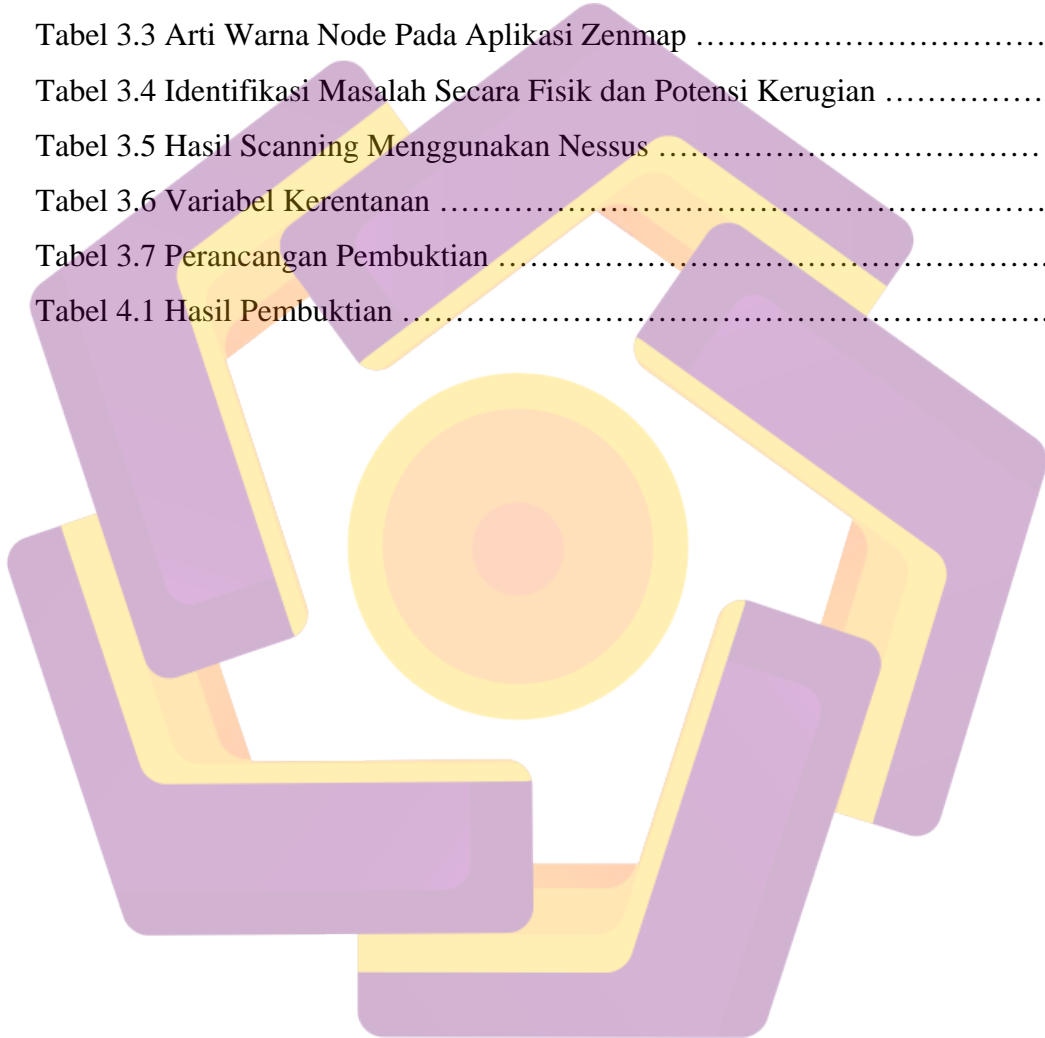
2.4.1	Intrusion	16
2.4.2	Denial of Service	17
2.4.3	Information Theft	19
2.4.4	Tipe Penyerang	22
2.5	Mekanisme Keamanan Server dan Jaringan	23
2.5.1	Firewall	23
2.5.2	Enkripsi	24
2.5.3	Intrusion Detection System (IDS)	25
2.5.4	Honeypot	25
2.6	Topologi Jaringan Komputer	26
2.7	Internet	28
2.7.1	Definisi Internet	28
2.7.2	Sejarah Internet	28
BAB III ANALISIS DAN PERANCANGAN SISTEM		29
3.1	Tinjauan Umum	29
3.2	Pre-engagement Interactions	30
3.2.1	Aspek Bisnis	30
3.2.2	Aspek Teknis	33
3.3	Persiapan Perangkat Uji	34
3.3.1	Menyiapkan Mesin Virtual	34
3.3.2	Menyiapkan Sistem Operasi	35
3.3.3	Zenmap	39
3.3.4	Instalasi Nessus	40
3.3.5	Metasploit	41
3.4	Intellegence Gathering	42
3.4.1	Kondisi LAN	42
3.4.2	Sistem Operasi Target	43
3.4.3	Layanan Tersedia	44
3.4.4	Observasi Lapangan	44
3.5	Vulnerability Analysis	46
3.6	Identifikasi Masalah	50
3.7	Threat Modelling	51
BAB IV IMPLEMENTASI DAN PEMBAHASAN		54



4.1	Exploitation	54
4.1.1	Eksploitasi Fisik	54
4.1.2	Eksploitasi FTP	59
4.1.3	Eksploitasi SSH	61
4.1.4	Eksploitasi Layanan Web Server	63
4.1.5	Eksploitasi Layanan Squid	65
4.1.6	Eksploitasi Otomatis dan Bruteforce	68
4.2	Reporting	71
4.2.1	Laporan Analisa Kerentanan	71
4.2.2	Laporan Eksploitasi	72
4.2.3	Laporan Pembuktian	72
4.2.4	Rekomendasi Pengamanan	73
BAB V	PENUTUP	76
5.1	Kesimpulan	76
5.2	Saran	77
DAFTAR PUSTAKA	78	
LAMPIRAN	80	

DAFTAR TABEL

Tabel 1.1 Jadwal Kegiatan	6
Tabel 2.1 Perbandingan Penelitian	7
Tabel 3.1 Persetujuan Pekerjaan Penetration Testing	31
Tabel 3.2 Spesifikasi Perangkat Keras di Warnet Galeri Informatika	33
Tabel 3.3 Arti Warna Node Pada Aplikasi Zenmap	42
Tabel 3.4 Identifikasi Masalah Secara Fisik dan Potensi Kerugian	44
Tabel 3.5 Hasil Scanning Menggunakan Nessus	48
Tabel 3.6 Variabel Kerentanan	50
Tabel 3.7 Perancangan Pembuktian	51
Tabel 4.1 Hasil Pembuktian	73



DAFTAR GAMBAR

Gambar 2.1 Topologi Star	27
Gambar 2.2 Topologi Hybrid	27
Gambar 3.1 Struktur Manajemen Warnet Galeri Informatika	29
Gambar 3.2 Topologi LAN Warnet Galeri Informatika	33
Gambar 3.3 Tampilan Oracle Virtual Box	34
Gambar 3.4 Membuat Mesin Virtual di Virtual Box	35
Gambar 3.5 Menentukan Kapasitas Hard Disk Mesin Virtual	36
Gambar 3.6 Setting Network Adapter Mesin Virtual	36
Gambar 3.7 Mengarahkan CD Drive Virtual ke Installer Sistem Operasi	36
Gambar 3.8 Menu Booting Live CD Kali Linux 1.0.6	37
Gambar 3.9 Tabel Partisi Hard Disk Pada Instalasi Kali Linux	37
Gambar 3.10 Tampilan Menu Booting Kali Linux	38
Gambar 3.11 Konfigurasi Jaringan Pada Kali Linux	38
Gambar 3.12 Percobaan Ping ke IP Address Publik Berhasil	39
Gambar 3.13 Antarmuka Zenmap	39
Gambar 3.14 Form Registrasi Nessus	40
Gambar 3.15 E-mail Kode Aktivasi Nessus	40
Gambar 3.16 Halaman Login Nessus Melalui Antarmuka Web	41
Gambar 3.17 Tampilan Metasploit Pada Terminal	41
Gambar 3.18 LAN Warnet Galeri Informatika	42
Gambar 3.19 OS Footprinting Menggunakan Zenmap	43
Gambar 3.20 Port yang Terbuka Pada Server Proxy	44
Gambar 3.21 Membuat Policy Scan	46
Gambar 3.22 Memilih Plugin untuk Scanning Vulnerability	47
Gambar 3.23 Memulai Scanning Nessus	48
Gambar 4.1 Tampak Dalam Klien nomor 5 Warnet	55
Gambar 4.2 Konfigurasi IP Address Dilihat Dari Command Prompt	55
Gambar 4.3 Properties LAN dapat Diakses Oleh User	56
Gambar 4.4 Port RJ 45 di Casing Belakang PC Klien	56
Gambar 4.5 Kabel UTP berhasil Dipindahkan ke Laptop	57
Gambar 4.6 Percobaan Ping ke Salah Satu Situs Internet	57

Gambar 4.7 Pencarian Modul dan Payload Untuk Eksploitasi FTP	59
Gambar 4.8 Eksploitasi FTP dengan Metasploit	60
Gambar 4.9 Pencarian Modul Eksploitasi SSH	61
Gambar 4.10 Eksploitasi SSH dengan Metasploit	62
Gambar 4.11 Pencarian Modul Eksploitasi Layanan Web Server	63
Gambar 4.12 Eksploitasi Web Server	64
Gambar 4.13 Eksploitasi Web Server	65
Gambar 4.14 Pencarian Modul Layanan Squid Proxy	66
Gambar 4.15 Memilih Payload untuk Eksploitasi Squid Proxy	66
Gambar 4.16 Eksploitasi Layanan Squid Proxy dengan Metasploit	67
Gambar 4.17 Tampilan Project Overview Metasploit	68
Gambar 4.18 Proses Scanning	69
Gambar 4.19 Proses Eksploitasi Otomatis	70
Gambar 4.20 Setting Parameter Task Bruteforce	70
Gambar 4.21 Hasil Akhir bruteforcing	71
Gambar 4.22 Mengunduh Laporan Otomatis dari Nessus	72
Gambar 4.24 Mengunduh Custom Report Metasploit	72
Gambar 4.25 IP Address dan MAC Filtering Pada Router	74

INTISARI

Dalam dunia jaringan komputer, proxy server dibutuhkan untuk manajemen sekaligus penghematan bandwidth. Proxy memiliki kemampuan untuk membuat cache data, sehingga request tidak selalu dilayani ke server utama. Sehingga pengguna di dalam jaringan tersebut merasa akses lebih cepat.

Dari sisi pengguna jaringan, ada kemungkinan seorang pengguna melakukan percobaan tindakan menyusup atau merusak sistem dengan memanfaatkan celah keamanan. Administrator jaringan, dalam hal ini pada Warnet Galeri Informatika, telah menyadari adanya pihak yang bermaksud merusak sistem. Ia pernah mendapati adanya percobaan login terhadap proxy servernya.

Tulisan ini membahas analisis keamanan pada proxy server. Vulnerability scanning dilakukan untuk mengetahui kerentanan dari sistem. Kemudian dilakukan pembuktian hasil analisis kerentanan dengan cara uji penetrasi. Pada kesimpulan, akan dipaparkan rekomendasi untuk menindaklanjuti hasil pembuktian.

Kata kunci: jaringan komputer, proxy, kerentanan, keamanan, uji penetrasi



ABSTRACT

In the world of computer networks, a proxy server is required for bandwidth savings also bandwidth management. Proxy has the ability to create a data cache, so the request is not always served to the main server. So, users in the network feel faster access.

From the users side, it is likely actions a user performs experiments infiltrate or damage a system by exploiting security holes. Network administrator, in this case the Warnet Galeri Informatika, has been aware of the party who intends to destroy the system. He never found the existence of the proxy server login attempts.

This paper discusses the security analysis on the proxy server. Vulnerability scanning is performed to determine the vulnerability of the system. Then do the verification results of the vulnerability analysis by means of the penetration test. In conclusion, the recommendation would be to follow up the results presented proof.

Keywords: *computer networking, proxy, vulnerability, security, penetration test*

