ANALISIS PERFORMA KEAMANAN JARINGAN DI PERUSAHAAN RITEL (STUDI KASUS: PT XYZ)

SKRIPSI

MUHAMMAD IRSYAD ABDURRAHMAN

NIM 2110511065

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2024

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul : Analisis Performa Keamanan Jaringan di Perusahaan Ritel (Studi Kasus: PT XYZ)

Nama : Muhammad Irsyad Abdurrahman

NIM : 2110511065

Disetujui oleh:

Penguji 1:

Henki Bayu Seta, S.Kom, MTI.

Penguji 2:

Nurhuda Maulana, S.T., M.T.

Pembimbing 1:

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM

Pembimbing 2:

Hamonangan Kinantan Prabu, S.T., M.T.

Diketahui oleh:

Koordinator Program Studi:
Dr. Widya Cholil, M.I.T
NIP. 221112080

Dekan Fakultas Ilmu Komputer:
Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM
NIP. 197605082003121002

Tanggal Ujian Tugas Akhir :
15 Januari 2025

LEMBAR PERSETUJUAN

LEMBAR PERSETUJUAN

Yang bertanda tangan di bawah ini:

Nama	: Muhammad Irsyad Abdurrahman
NIM	: 2110511065
Program Studi	: Informatika
Judul Skripsi/TA	: Analisis Performa Keamanan Jaringan di Perusahaan Ritel (Studi Kasus: PT XYZ)

Dinyatakan telah memenuhi syarat dan menyetujui untuk mengikuti ujian sidang skripsi/tugas akhir.

Jakarta, 12 Desember 2024

Menyetujui,

Dosen Pembimbing I,	Dosen Pembimbing II,
Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM	Hamonangan Kinantan Prabu, S.T, M.T.

Mengetahui,

Ketua Program Studi,

Dr. Widya Cholil, S.Kom., M.I.T.

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama	: Muhammad Irsyad Abdurrahman
NIM	: 2110511065
Tanggal	: 22 Januari 2025

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Januari 2025

Yang Menyatakan

Muhammad Irsyad Abdurrahman

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Irsyad Abdurrahman
NIM	: 2110511065
Fakultas	: Ilmu Komputer
Program Studi	: S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (Non - exclusive Royalty Free Right) atas skripsi saya yang berjudul:

Analisis Performa Keamanan Jaringan di Perusahaan Ritel (Studi Kasus: PT XYZ)

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta

Pada tanggal: 22 Januari 2025

Yang Menyatakan

Muhammad Irsyad Abdurrahman

ABSTRAK

Pertumbuhan terhadap serangan DDoS dan serangan *ransomware* pada industri ritel meningkat di beberapa tahun terakhir. Berdasarkan laporan Verizon pada tahun 2023, *Denial-of-Service* dan *Ransomware* menjadi insiden yang paling sering terjadi. Salah satu cara untuk memitigasi serangan tersebut adalah dengan meningkatkan keamanan jaringan. Kontrol keamanan pada jaringan dapat berupa penerapan *firewall*, *honeypot*, IDS, dan *proxy*. Penelitian ini mencoba untuk menganalisis dan menguji performa keamanan jaringan pada PT XYZ terhadap serangan DDoS dan serangan *ransomware*, serta merancang mitigasi serangan DDoS dan serangan *ransomware* pada PT XYZ dengan kontrol keamanan yang baru. Penelitian dilakukan pada *security testing environment* yang menyerupai lingkungan pada PT XYZ agar tidak mengganggu operasional bisnis perusahaan. Penerapan *firewall* dan *reverse proxy* untuk memitigasi serangan DDoS berhasil dilakukan dan hasilnya kontrol keamanan tersebut mampu mengurangi *impact* dari serangan dengan *flag* SYN, TCP, dan HTTP dengan perubahan rata-rata kenaikan pada *throughput* sebesar 6,67 Mbps, rata-rata nilai pada *jitter* sebesar 2,23 ms, rata-rata persentase penurunan *latency* sebesar 86,67%, rata-rata persentase penurunan *packet loss* sebesar 87%, dan rata-rata persentase penurunan penggunaan CPU pada *firewall* sebesar 49,67%. Selain itu, penerapan Suricata sebagai IDS juga mampu mendeteksi adanya serangan DDoS dan serangan *ransomware* dengan *rule* dari ET Open.

Kata kunci: keamanan jaringan, *ransomware*, DDoS, *firewall*, *honeypot*, Suricata, ritel

ABSTRACT

The retail industry has seen a significant rise in DDoS and ransomware attacks over recent years. According to Verizon's 2023 report, Denial-of-Service and ransomware rank among the most frequent incidents. Strengthening network security is one of the key strategies to mitigate these threats. Security measures such as firewalls, honeypots, IDS, and proxies are essential components. This study aims to analyze and evaluate the performance of network security at PT XYZ in responding to DDoS and ransomware attacks while designing new mitigation strategies. The research was conducted in a security testing environment that simulates PT XYZ's operational setup, ensuring no disruption to business operations. The implementation of firewalls and reverse proxies successfully mitigated DDoS attacks, demonstrating their ability to reduce the impact of such threats involving SYN, TCP, and HTTP flags resulted in an average throughput increase of 6.67 Mbps, an average jitter value of 2.23 ms, a significant 86.67% decrease in latency, an 87% reduction in packet loss, and a 49.67% drop in CPU usage on the firewal.. Additionally, Suricata was employed as an IDS and effectively detected both DDoS and ransomware attacks using ET Open rules.

Keywords: *network security*, *ransomware*, DDoS, *firewall*, *honeypot*, Suricata, *retail*

KATA PENGANTAR

Puji dan syukur peneliti haturkan kehadirat Allah SWT, karena berkat rahmat dan hidayah-Nya-lah peneliti dapat menyelesaikan skripsi yang berjudul "Analisis Performa Keamanan Jaringan di Perusahaan Ritel (Studi Kasus: PT XYZ)". Skripsi ini dibuat untuk memenuhi tugas akhir perkuliahan dan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Strata 1 di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta. Selain itu, skripsi ini juga dibuat sebagai salah satu wujud implementasi dari ilmu yang didapatkan oleh peneliti selama masa perkuliahan di Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Skripsi ini tentunya tidak lepas dari bimbingan, masukan, dan arahan dari berbagai pihak. Oleh karena itu, pada kesempatan ini peneliti ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Allah SWT. yang telah memberikan karunia, rahmat, dan hidayah-Nya selama peneliti menyelesaikan skripsi penelitian ini.
2. Abi dan Umi selaku orangtua peneliti, yang merupakan sumber inspirasi, doa, dan *support system* terbesar peneliti dan yang selalu menemani peneliti di masa sulit.
3. Ibu Dr. Widya Cholil, S.Kom., M.I.T. selaku Ketua Program Studi Sarjana Jurusan Informatika dan jajarannya yang telah memfasilitasi dan mendukung kelancaran proses penyelesaian skripsi penelitian ini.
4. Bapak Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM selaku dosen pembimbing pertama yang telah mengarahkan dan membimbing peneliti sekaligus sosok yang menginspirasi peneliti untuk meneliti topik skripsi yang peneliti angkat.
5. Bapak Hamonangan Kinantan Prabu, S.T, M.T. selaku dosen pembimbing kedua, yang telah meluangkan waktu untuk memberikan masukan dan saran

dalam segi penulisan, maupun teknis proses penyusunan skripsi penelitian ini.

6. Ibu Neny Rosmawarni, M.Kom. sebagai dosen pembimbing akademik dan yang telah memberikan dukungan dan motivasi dalam menyelesaikan skripsi ini sekaligus sosok yang memberikan kontribusi besar terhadap perjalanan akademik peneliti.
7. Mba Upat, Mas Ojan, Mas Iam, Mba Pipah, dan saudara-saudari yang telah menjadi bagian dari kehidupan peneliti dan selalu membantu peneliti dalam kondisi susah maupun bahagia.
8. Teman-teman *server* Discord KYUT yang selalu ada untuk mendukung dan menemani peneliti dalam perjalanan kehidupan peneliti di FIK UPN Veteran Jakarta.
9. Tachibana Hinano, karakter Vtuber Jepang dari agensi VSPO!, selaku salah satu *support system* peneliti sehingga peneliti dapat termotivasi secara emosinal dan mental untuk menyelesaikan skripsi penelitian.
10. Semua pihak yang telah membantu dan tidak dapat peneliti sebutkan satu persatu.

Skripsi ini diketik dan disusun ketika peneliti sedang mengalami musibah dan cobaan sehingga peneliti sangat-sangat berterima kasih kepada semua pihak yang telah membantu peneliti dalam menyelesaikan penelitian ini. Tanpa adanya kehadiran mereka, peneliti merasa kesulitan untuk menghadapi tantangan dan cobaan yang sedang dialami. Peneliti sadar bahwa musibah ini adalah suatu ujian dari Allah SWT untuk selalu taat beribadah kepada-Nya dan selalu bersyukur kapan pun dan di mana pun. Peneliti juga ingin mengingatkan kepada para pembaca untuk selalu bersyukur setiap saat, jangan pernah putus asa, dan percaya bahwa semuanya akan baik-baik saja selama kita tetap berusaha, berserah diri kepada Yang Maha Kuasa, dan memberikan yang terbaik untuk segalanya.

Peneliti menyadari skripsi ini masih belum sempurna, baik dari materi, penelitian, maupun dari segi penyajian karena keterbatasan pengetahuan dan

kemampuan peneliti. Oleh karena itu, peneliti sangat mengharapkan saran dan kritik untuk kesempurnaan skripsi ini.

Jakarta, Oktober 2024

Peneliti

Muhammad Irsyad Abdurrahman

DAFTAR ISI

LEMBAR PENGESAHAN i
LEMBAR PERSETUJUAN ii
PERNYATAAN ORISINALITAS iii
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS iv
ABSTRAK v
ABSTRACT vi
KATA PENGANTAR vii
DAFTAR ISI x
DAFTAR GAMBAR xiii
DAFTAR TABEL xvi
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 3
1.3. Tujuan Penelitian 3
1.4. Batasan Masalah 3
1.5. Luaran yang Diharapkan 4
1.6. Sistematika Penelitian 4
BAB II LANDASAN TEORI 6
2.1. Keamanan Jaringan 6
2.2. Ancaman terhadap Keamanan Jaringan 7
2.2.1. Ancaman Internal 7
2.2.2. Ancaman Eksternal 7
2.3. Serangan Ransomware 9
2.3.1. Jenis Ransomware 9
2.3.2. Cara Kerja Serangan Ransomware 10
2.4. Serangan DDoS 12
2.4.1. Jenis Serangan DoS terhadap Jaringan 13
2.5. Mitigasi Serangan Keamanan Jaringan 14
2.5.1. Desain Jaringan 15
2.5.2. Firewall 15
2.5.3. Intrusion Detection Prevention System (IDPS) 17

2.5.4. Honeypot 18
2.5.5. Security Testing Environment 18
2.5.6. Whitebox Testing 18
2.6. Perusahaan Ritel 19
2.6.1. Jenis Perusahaan Ritel 19
2.6.2. Infrastruktur Jaringan Perusahaan Ritel 21
2.6.3. Aplikasi yang digunakan pada Perusahaan Ritel 22
2.7. Literature Review 22
BAB III METODE PENELITIAN 28
3.1. Tahapan Penelitian 28
3.1.1. Studi Literatur dan Pustaka 29
3.1.2. Pendefinisian Masalah dan Kebutuhan Sistem 29
3.1.3. Audit Sistem 29
3.1.4. Perancangan Mitigasi Serangan 30
3.1.5. Uji Coba 31
3.1.6. Evaluasi Sistem 32
3.1.7. Mengambil Kesimpulan 32
3.1.8. Dokumen dan Laporan 32
3.2. Flowchart Perancangan Sistem dan Uji Coba 33
3.3. Analisis Kebutuhan 34
3.4. Waktu dan Tempat 34
3.5. Jadwal Kegiatan 35
BAB IV HASIL PEMBAHASAN 36
4.1. Analisis Jaringan PT XYZ 36
4.2. Sistem Keamanan Jaringan Data Center 38
4.2.1. Threat Modelling 38
4.2.2. Rancangan Sistem Keamanan yang Diusulkan 40
4.2.3. Implementasi Sistem Keamanan 41
4.3. Sistem Keamanan Jaringan Head Office 55
4.3.1. Threat Modelling 55
4.3.2. Rancangan Sistem Keamanan yang Diusulkan 58
4.3.3. Implementasi Sistem Keamanan 59
4.4. Pengujian Sistem Keamanan 67
4.4.1. Sistem Keamanan Jaringan Data Center 67

4.4.2. Sistem Keamanan Jaringan Head Office..... 72
4.5. Analisis Performa Sistem Keamanan.....74
4.5.1. Performa Jaringan Data Center 74
4.5.2. Performa Jaringan Head Office..... 87
BAB V KESIMPULAN.....93
5.1. Kesimpulan 93
5.2. Saran.....94
DAFTAR PUSTAKA 95
LAMPIRAN.....98

DAFTAR GAMBAR

Gambar 2.1 Tahapan serangan *ransomware* 12
Gambar 2.2 Skema penyerangan DDoS 13
Gambar 2.3 Ilustrasi *Defense-in-Depth* 15
Gambar 3.1 Flowchart Tahapan Penelitian 28
Gambar 3.2 Flowchart perancangan sistem 33
Gambar 4.1 Topologi Jaringan pada PT XYZ 37
Gambar 4.2 *Threat modelling* pada *flow data* dari dan menuju VMS. 39
Gambar 4.3 Rancangan Mitigasi Serangan DDoS 41
Gambar 4.4 Fortigate 81F di Data Center 43
Gambar 4.5 Contoh *rule* dari Suricata 45
Gambar 4.6 Tampilan antarmuka awal T-Pot 52
Gambar 4.7 Versi dari Apache yang digunakan 54
Gambar 4.8 Versi dari iperf3 yang digunakan 55
Gambar 4.9 *Threat Modelling* pada *flow data* dari karyawan menuju internet 56
Gambar 4.10 Hierarki akses pada domain tertentu untuk karyawan 57
Gambar 4.11 Rancangan mitigasi serangan *ransomware* 59
Gambar 4.12 Diagram skenario serangan DDoS pada *security testing environment* 59
Gambar 4.13 Sebagian domain pada daftar domain blacklist_squid.acl 62
Gambar 4.14 *Rules* yang digunakan pada Rule Emerging Threat 64
Gambar 4.15 *Ransomware* yang disimpan pada server 65
Gambar 4.16 Konfigurasi *proxy* pada PC User 66
Gambar 4.17 Topologi Jaringan terbaru dengan penambahan kontrol keamanan 66
Gambar 4.18 Pengujian performa jaringan pada skenario ke-1 70
Gambar 4.19 Pengujian performa jaringan pada skenario ke-2 71
Gambar 4.20 Pengujian performa jaringan pada skenario ke-3 71
Gambar 4.21 Pengujian performa jaringan pada skenario ke-4 72

Gambar 4.22 Contoh tampilan dari hasil pengujian dengan fast.com 73
Gambar 4.23 Tampilan dari tmNIDS.....74
Gambar 4.24 VM Monitoring gagal untuk melakukan koneksi TCP ke *firewall* 76
Gambar 4.25 VM Monitoring gagal untuk melakukan koneksi UDP ke *firewall* 76
Gambar 4.26 Hasil deteksi Suricata terhadap serangan SYN *flood*.....77
Gambar 4.27 Hasil deteksi Suricata terhadap serangan TCP *flood* 78
Gambar 4.28 Hasil deteksi Suricata terhadap serangan HTTP *flood*.....78
Gambar 4.29 Hasil deteksi Suricata setelah *client* terkena *rate limit* 79
Gambar 4.30 Diagram batang perbandingan *throughput* setiap skenario.....80
Gambar 4.31 Diagram batang perbandingan *jitter* setiap skenario.....81
Gambar 4.32 Diagram batang perbandingan *latency* setiap skenario.....82
Gambar 4.33 Diagram batang perbandingan *packet loss* setiap skenario.....83
Gambar 4.34 Diagram batang perbandingan penggunaan CPU setiap skenario 84
Gambar 4.35 Tampilan aplikasi web SNARE/Tanner sebagai *honeypot* 85
Gambar 4.36 Tampilan *dashboard* Tanner sebagai *honeypot* 85
Gambar 4.37 Penggunaan sumber daya pada server T-Pot 87
Gambar 4.38 Perbandingan kecepatan internet sebelum dan sesudah menerapkan kontrol keamanan 88
Gambar 4.39 Tampilan pemblokiran akses ke domain ransomware-server.com oleh Squid Proxy.....89
Gambar 4.40 Tampilan ketika mengakses internet dengan autentikasi pada browser.....90
Gambar 4.41 Hasil deteksi Suricata terhadap User-Agent yang mencurigakan 91
Gambar 4.42 Hasil deteksi Suricata terhadap DNS tor dan koneksi IP yang berbahaya 91
Gambar 4.43 Hasil deteksi Suricata terhadap unduhan file EXE melalui HTTP 91

Gambar 4.44 Hasil deteksi Suricata terhadap *lookup* alamat IP eksternal.....92
Gambar 4.45 Hasil deteksi Suricata terhadap aktivitas *ransomware* Cerber..92

DAFTAR TABEL

Tabel 2.1 Penelitian terdahulu 23
Tabel 3.1 Skenario uji coba untuk performa jaringan.....31
Tabel 3.2 Jadwal Kegiatan Penelitian.....35
Tabel 4.1 Spesifikasi VM Sistem Keamanan Jaringan Data Center.....42
Tabel 4.2 Daftar *honeypot* pada *framework* T-Pot.....52
Tabel 4.3 Spesifikasi VM Sistem Keamanan Jaringan Head Office 60
Tabel 4.4 Hasil performa jaringan dari pengujian setiap skenario 75