Simulasi Serangan Siber dan Pengujian Jaringan pada Sistem NIDS Berbasis Snort di Lingkungan Ubuntu Server

Fitra Maulana

D4 Teknologi Rekayasa Internet · Sekolah Vokasi · Universitas Gadjah Mada · 2024

Praktik Industri · PT TechnoGIS Indonesia (Jagoweb) · 27 Juni – 10 Agustus 2024

fitramaulana@mail.ugm.ac.id · gitlab.com/maulanafitra

Abstrak

Dokumen ini mendeskripsikan kontribusi penulis dalam proyek Praktik Industri bersama PT TechnoGIS Indonesia yang berfokus pada pengembangan sistem monitoring serangan siber berbasis Snort NIDS di lingkungan Ubuntu Server. Kontribusi penulis mencakup perancangan topologi jaringan, konfigurasi router MikroTik sebagai pusat infrastruktur jaringan pengujian, serta eksekusi seluruh skenario simulasi serangan siber menggunakan Kali Linux sebagai platform penyerang. Serangan yang disimulasikan meliputi Port Scanning (Nmap: Basic, TCP ACK, FIN, Null Scan), Denial of Service (Hping3: SYN flood, ICMP flood, UDP flood), dan Brute Force SSH (Hydra). Seluruh vektor serangan berhasil dieksekusi dan divalidasi melalui log deteksi Snort dengan tingkat efektivitas deteksi 100% serta Wireshark 96%.

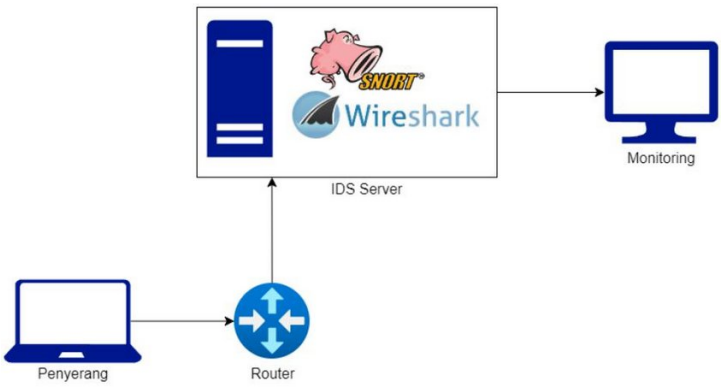
Kata Kunci: *Cybersecurity, Network Intrusion Detection System, Snort, Kali Linux, MikroTik, Penetration Testing, Simulasi Serangan Siber*

I. Pendahuluan

Keamanan infrastruktur jaringan menjadi aspek kritis dalam operasional sistem digital modern. Network-based Intrusion Detection System (NIDS) merupakan salah satu pendekatan proaktif untuk memantau dan mendeteksi anomali lalu lintas jaringan secara real-time. Snort, sebagai NIDS berbasis open-source, telah menjadi pilihan utama dalam implementasi keamanan jaringan di berbagai lingkungan produksi.

Proyek Praktik Industri ini dilaksanakan di PT TechnoGIS Indonesia (divisi Jagoweb) selama 1,5 bulan (27 Juni – 10 Agustus 2024) sebagai proyek tim bersama Rangga Wiguna. Dalam proyek tim ini, penulis bertanggung jawab atas dua aspek utama: (1) perancangan dan implementasi infrastruktur jaringan pengujian menggunakan router MikroTik, serta (2) eksekusi seluruh skenario simulasi serangan siber menggunakan Kali Linux untuk memvalidasi efektivitas sistem deteksi yang dibangun oleh rekan tim.

II. Lingkungan dan Infrastruktur Jaringan



Proyek menggunakan topologi jaringan seperti pada gambar diatas dengan router MikroTik hAP sebagai pusat jaringan. Seluruh perangkat terhubung melalui router yang berfungsi sebagai switch dan gateway internet. Penulis merancang dan mengimplementasikan seluruh konfigurasi jaringan berikut:

A. Spesifikasi Perangkat

Perangkat	Spesifikasi	Peran
Router MikroTik	hAP RB951Ui-2HnD, 600MHz, 128MB RAM	Network hub, DHCP server, NAT gateway
PC Penyerang	AMD Ryzen 5 3500U, 8GB RAM, Kali Linux	Platform serangan (kontribusi penulis)
PC Server	AMD Ryzen 7 5800H, 16GB RAM, Ubuntu 18.04	Target serangan & IDS (rekan tim)

B. Addressing Table Jaringan

Device	Interface	IP Address	Subnet Mask	Gateway
Router	Wlan1	192.168.12.156	255.255.255.0	192.168.12.1
Router	Bridge	192.168.22.1	255.255.255.0	192.168.22.1
Server	NIC	192.168.22.252	255.255.255.0	192.168.22.1
Kali Linux	NIC	192.168.22.253	255.255.255.0	192.168.22.1

C. Konfigurasi MikroTik yang Diimplementasikan

Berikut langkah konfigurasi MikroTik yang dilakukan penulis:

- **Identity & Security Profile:** Mengonfigurasi identitas router dan profil keamanan WPA2 PSK untuk koneksi wireless terenkripsi.
- **Wireless Interface (wlan1 & wlan2):** Konfigurasi wlan1 sebagai Station Pseudobridge ke jaringan utama, dan wlan2 sebagai AP Bridge untuk jaringan lokal pengujian.
- **Bridge Configuration:** Menggabungkan interface ether2-5 dan wlan2 ke dalam bridge1 sebagai satu segmen jaringan.
- **DHCP Server & Client:** DHCP client pada wlan1 untuk mendapat IP dari ISP; DHCP server pada bridge1 untuk mendistribusikan IP ke Kali Linux dan Ubuntu Server secara otomatis.
- **NAT Masquerade:** Firewall rule masquerade pada chain srcnat agar perangkat lokal dapat mengakses internet melalui IP ISP.
- **Konektivitas Validasi:** Uji koneksi menggunakan ping ke 8.8.8.8 (Google DNS) dan antar perangkat lokal — seluruh koneksi berhasil.

II. Metodologi Simulasi Serangan

Penulis mengeksekusi tiga kategori utama simulasi serangan siber dari mesin Kali Linux (192.168.22.253) yang menargetkan Ubuntu Server (192.168.22.252). Pemilihan vektor serangan dirancang untuk menguji spektrum ancaman dari reconnaissance hingga access attempt.

A. Port Scanning dengan Nmap

Port scanning digunakan untuk mengidentifikasi port terbuka dan pemetaan layanan aktif pada target. Penulis mengeksekusi empat teknik scanning:

Teknik	Perintah	Tujuan
Basic Scan	nmap 192.168.22.252	Identifikasi port terbuka dasar
TCP ACK Scan	nmap -sA -T4 192.168.22.252/24	Deteksi filtering firewall
FIN Scan	nmap -sF -T4 192.168.22.252/24	Bypass firewall stateful
Null Scan	nmap -sN -T4 192.168.22.252/24	Stealth scan tanpa TCP flag

B. Denial of Service (DoS) Attack dengan Hping3

Serangan DoS bertujuan menghabiskan resource server sehingga layanan tidak dapat diakses. Penulis menggunakan Hping3 untuk mensimulasikan tiga jenis flood attack:

Jenis	Perintah	Mekanisme
SYN Flood	hping3 -S --flood -p 22 192.168.22.252	Banjiri half-open TCP connections
ICMP Flood	hping3 --icmp --flood -v -p 22 192.168.22.252	Banjiri ICMP ping requests
UDP Flood	hping3 --udp --flood -v -p 22 192.168.22.252	Banjiri port 22 dengan paket UDP

C. Brute Force SSH dengan Hydra

Teknik brute force digunakan untuk menguji ketahanan autentikasi SSH server terhadap percobaan login masif menggunakan wordlist username dan password:

- **Perintah:** hydra -L user.txt -P password.txt ssh://192.168.22.252 -t 4
- **Hasil:** Hydra berhasil menemukan kombinasi username *proyek* dan password *12345* — mengkonfirmasi kerentanan penggunaan kredensial lemah pada layanan SSH.

III. Hasil Validasi Serangan

Seluruh serangan yang dieksekusi penulis berhasil dideteksi oleh sistem NIDS (Snort) dan dianalisis menggunakan Wireshark oleh rekan tim. Berikut ringkasan hasil deteksi:

Vektor Serangan	Snort Rule SID	Pesan Alert	Snort	Wireshark
Nmap Basic/MAP Scan	1000001	MAP scan detected	✓	✓
TCP ACK Scan	1000002	ACK Scan Detected	✓	✓
FIN Scan	1000003	FIN scan detected	✓	✓
Null Scan	1000004	Null scan detected	✓	✓
SYN Flood	1000009	Possible SYN Flood Attack	✓	✓
ICMP Flood	1000006	ICMP flood detected	✓	✓
UDP Flood	1000007	UDP flood detected	✓	✓
SSH Brute Force	1000020	Potential SSH Brute Force Attack	✓	✓

Snort mencatat efektivitas deteksi 100% — seluruh pola serangan terdeteksi dan dicatat dalam log sesuai rules yang dikonfigurasi. Wireshark mencatat efektivitas 96% — terdapat force close sesekali saat volume serangan DoS sangat tinggi.

IV. Kesimpulan

Proyek ini membuktikan bahwa perancangan topologi jaringan yang tepat dan kemampuan eksekusi simulasi serangan siber yang komprehensif merupakan komponen kritis dalam validasi efektivitas sistem NIDS.

Dari sisi penulis, proyek ini memberikan pengalaman langsung dalam: konfigurasi infrastruktur jaringan berbasis MikroTik pada lingkungan produksi, pemahaman mendalam tentang anatomi serangan siber dari perspektif penyerang (offensive security mindset), serta kemampuan mereplikasi berbagai teknik penetration testing yang digunakan oleh profesional keamanan jaringan.

Kombinasi NIDS berbasis Snort yang dikombinasikan dengan Wireshark terbukti efektif sebagai solusi monitoring keamanan jaringan pada lingkungan on-premise, dengan kemampuan mendeteksi berbagai vektor ancaman mulai dari reconnaissance hingga exploitation attempts secara real-time.