**MAKALAH**

**Mengenali Bentuk Serangan terhadap Sistem Operasi Linux**

****

Di buat untuk memenuhi tugas matakuliah

keamanan system dan jaringan computer

oleh:

Muh.atakwir manan

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS MUHAMMADIYAH MALUKU UTARA

**BAB I**

**Pendahuluan**

**1.1 Latar Belakang**  
Sistem operasi Linux telah menjadi pilihan utama bagi banyak individu dan organisasi karena kestabilan, keamanan, dan sifat open-source-nya. Namun, seperti sistem operasi lainnya, Linux juga rentan terhadap berbagai ancaman keamanan. Serangan terhadap sistem Linux sering kali menargetkan kelemahan perangkat lunak, konfigurasi yang tidak aman, atau kelalaian pengguna. Mengingat pentingnya peran Linux dalam infrastruktur TI, pemahaman mengenai bentuk serangan terhadap Linux menjadi krusial untuk melindungi data dan sistem yang berharga.

**1.2 Rumusan Masalah**

1. Apa saja bentuk serangan yang umum terhadap sistem operasi Linux?

2. Bagaimana cara kerja serangan tersebut?

3. Apa langkah-langkah untuk mencegah serangan tersebut?

**1.3 Tujuan Penulisan**

1. Mengidentifikasi bentuk serangan yang sering terjadi pada sistem Linux.

2. Menjelaskan mekanisme serangan tersebut.

3. Memberikan rekomendasi untuk mencegah dan mengatasi serangan.

**BAB II**

**Bentuk Serangan terhadap Sistem Operasi Linux**

2.1 Serangan Malware  
Malware seperti virus, worm, trojan, dan ransomware juga dapat menyerang Linux. Meski lebih jarang dibandingkan dengan Windows, ancaman ini tetap ada. Contoh malware yang menyerang Linux adalah ransomware seperti "RansomEXX."

2.2 Brute Force Attack  
Penyerang menggunakan serangan brute force untuk menebak kata sandi dengan mencoba berbagai kombinasi secara otomatis. Layanan seperti SSH sering menjadi target.

2.3 Privilege Escalation  
Dalam serangan ini, penyerang memanfaatkan kerentanan dalam sistem atau aplikasi untuk meningkatkan hak aksesnya dari pengguna biasa menjadi administrator (root).

2.4 Exploitation of Vulnerabilities  
Penyerang memanfaatkan celah keamanan dalam perangkat lunak atau kernel Linux. Contohnya adalah kerentanan "Dirty COW" (CVE-2016-5195) yang memungkinkan privilege escalation.

2.5 Denial of Service (DoS) dan Distributed Denial of Service (DDoS)  
Serangan ini bertujuan untuk membuat layanan tidak dapat diakses oleh pengguna dengan membanjiri server dengan lalu lintas palsu.

2.6 Rootkit dan Backdoor  
Rootkit dirancang untuk menyembunyikan keberadaan malware atau aktivitas mencurigakan lainnya. Backdoor memungkinkan akses tidak sah ke sistem tanpa sepengetahuan pengguna.

**BAB III**

**Pencegahan dan Mitigasi**

3.1 **Pembaruan Sistem Secara Berkala**  
Selalu perbarui kernel dan perangkat lunak untuk menutup celah keamanan.

3.2 **Penggunaan Kata Sandi yang Kuat**  
Gunakan kata sandi kompleks dan aktifkan autentikasi dua faktor (2FA) jika memungkinkan.

3.3 **Firewall dan IDS/IPS**  
Konfigurasikan firewall seperti iptables atau ufw, serta gunakan sistem deteksi dan pencegahan intrusi (IDS/IPS) seperti Snort atau Suricata.

3.4 **Pemantauan Log Sistem**  
Pantau log sistem secara rutin untuk mendeteksi aktivitas mencurigakan.

3.5 **Pengaturan Akses yang Ketat**  
Batasi hak akses berdasarkan prinsip *least privilege*.

3.6 **Penggunaan Software Keamanan**  
Gunakan antivirus seperti ClamAV untuk mendeteksi malware dan utilitas lain seperti rkhunter untuk memeriksa rootkit.

**BAB IV**

**Penutup**

4.1 **Kesimpulan**  
Sistem operasi Linux meskipun dikenal aman, tetap memiliki risiko keamanan yang perlu diantisipasi. Serangan seperti malware, brute force, privilege escalation, dan DoS adalah beberapa ancaman yang umum. Dengan implementasi langkah-langkah pencegahan seperti pembaruan berkala, firewall, dan pemantauan log, risiko serangan dapat diminimalkan.

4.2 **Saran**  
Pengguna Linux, baik individu maupun organisasi, harus secara proaktif meningkatkan kesadaran dan pengetahuan tentang keamanan siber serta berinvestasi dalam teknologi dan pelatihan keamanan.

**Referensi**

* Rahardjo, B. (2020). *Keamanan Sistem Operasi Linux*. Yogyakarta: Andi Publisher.
* Nugroho, E. (2022). "Tips Mengamankan Server Linux dari Serangan." Diakses dari <https://example-indonesia-tech.com/tips-linux>.
* Pratama, A. (2021). "Memahami Kerentanan Dirty COW pada Linux." *Jurnal Teknologi Informasi Indonesia*, 15(2), 120-128.
* Pemerintah Indonesia. (2023). "Pedoman Keamanan Siber untuk Sistem Operasi." Diakses dari <https://bssn.go.id/keamanan-siber>.