PROGRESS

CYBER NOIR

SYSTEM

SYSTEM STATUS: SECURE
KERNEL INTEGRITY: OK
THREAT LEVEL: LOW
NETWORK: ENCRYPTED

Linux ve Siber Güvenlik: Mimari, Riskler ve Savunma

İşletim Sistemi Temellerinden Kernel Exploit'lere Derinlemesine Bir Bakış

> $ sudo iptables -L

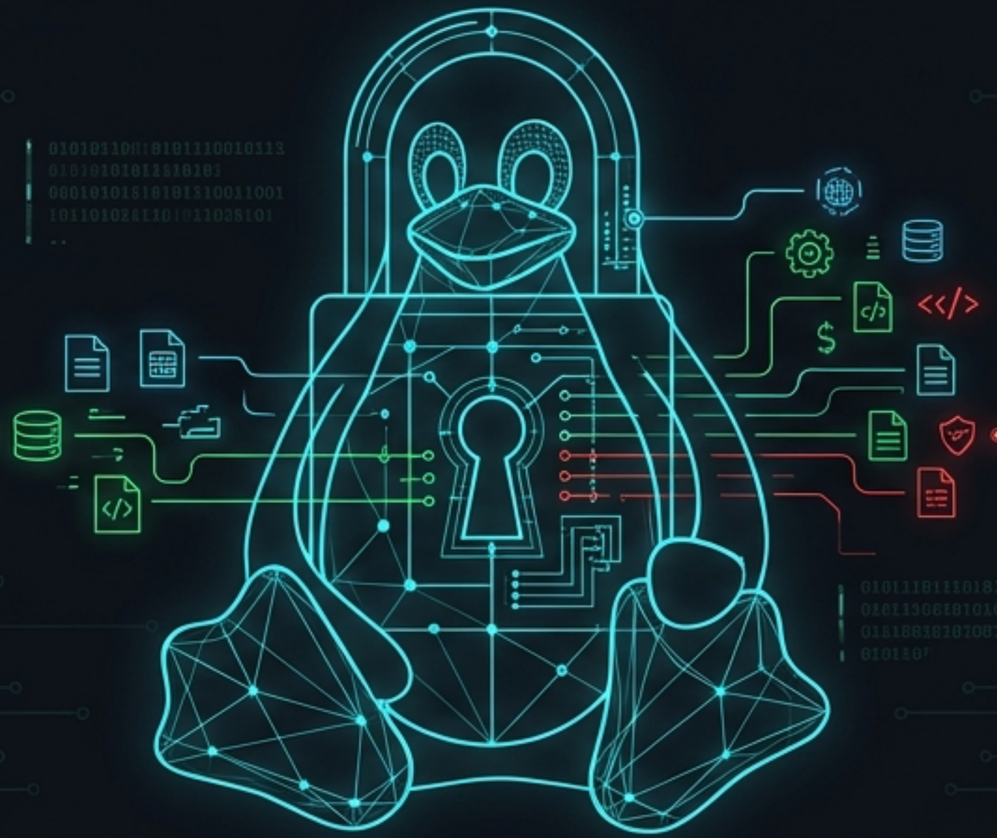
LINUX MIMARİSİ

USER SPACE
(Applications, Libraries)

KERNEL SPACE

- System Calls
- Device Drivers
- File System
- Networking
- Process Management

HARDWARE



> $ grep -r 'CVE' *

SİBER RİSKLER & SAVUNMA

RISK TYPES
(Malware
Kernel Exploits
Buffer Overflows
Privilege Escalation)

DEFENSE MECHANISMS
(SELinux/AppArmor
Secure Boot
ASLR/DEP
Kernel Hardening
Auditing)

> $ grep -r 'CVE' *

Temeller: Açık Kaynak Felsefesi

- **Güvenlik ve Şeffaflık:** Kodun denetlenebilirliği esastır.
- **Tarihçe:** 1991, Linus Torvalds ve GNU araçları.
- **Dominasyon:** Sunucuların ve güvenlik araçlarının %90'ı.
- **Topluluk Gücü:** Hızlı yama (patch) ve CVE takibi.

Kali Linux

Saldırı & Test

- Penetrasyon Testleri (Pentest)
- Offensive Security
- 600+ Hazır Araç

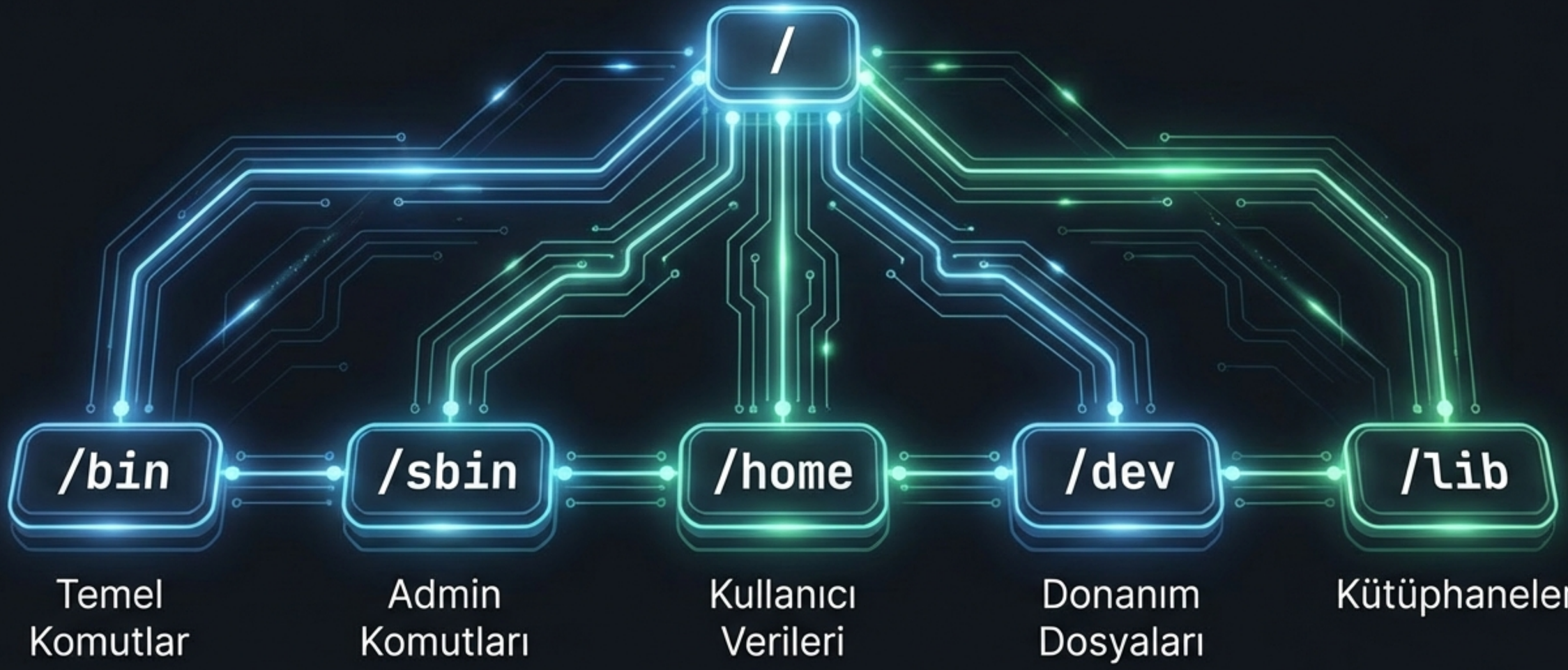
Parrot Security OS

Savunma & Analiz

- Adli Bilişim (Forensics)
- Gizlilik Odaklı
- Hafif Mimari

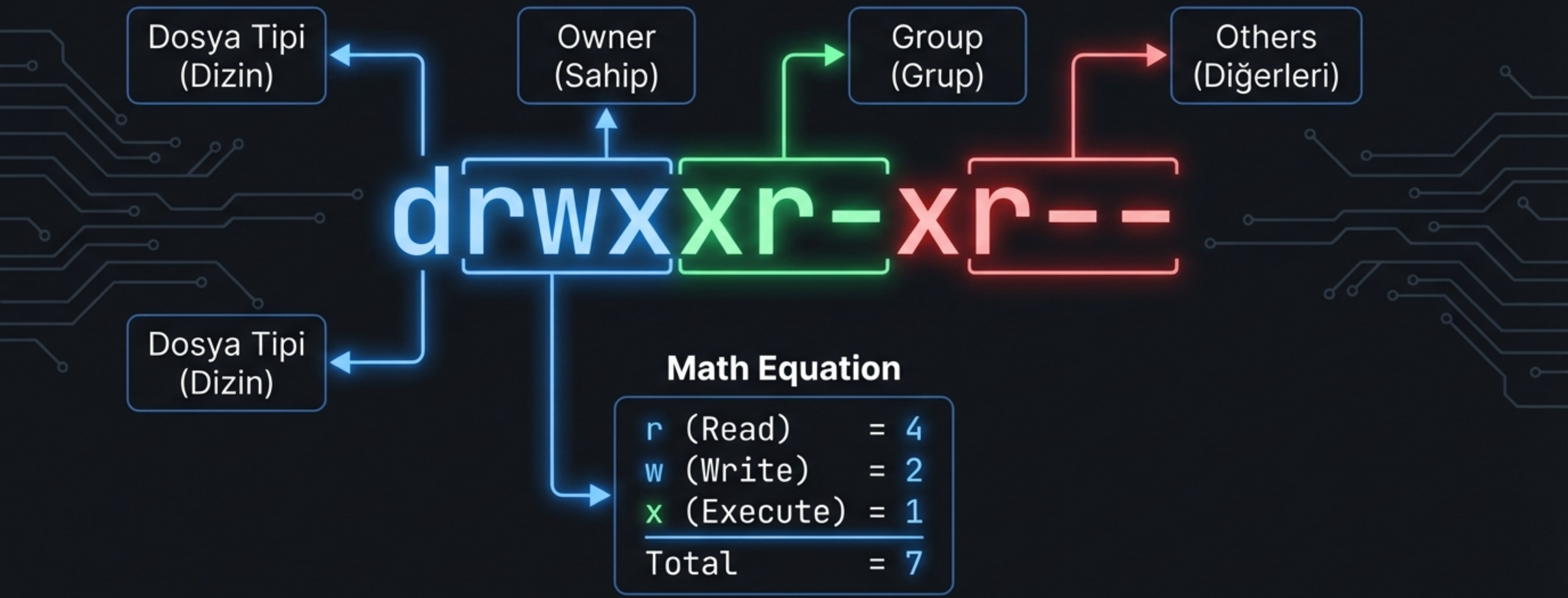
Harita: Dosya Sistemi Hiyerarşisi (FHS)

Linux'ta her şey bir dosyadır.

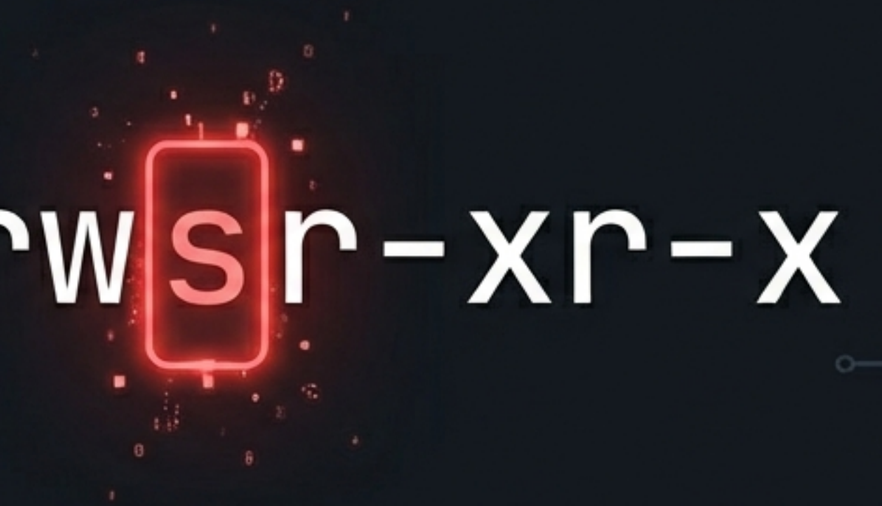


Kritik Bölgeler: Hedef ve Risk Noktaları

Kapı Bekçileri: Dosya İzinleri



Gizli Tehlikeler: Özel İzinler



SUID (SetUID)

Dosya, çalıştıranın değil, sahibinin (**Root**) yetkisiyle çalışır. **Yanlış** yapılandırma = **Privilege Escalation**.

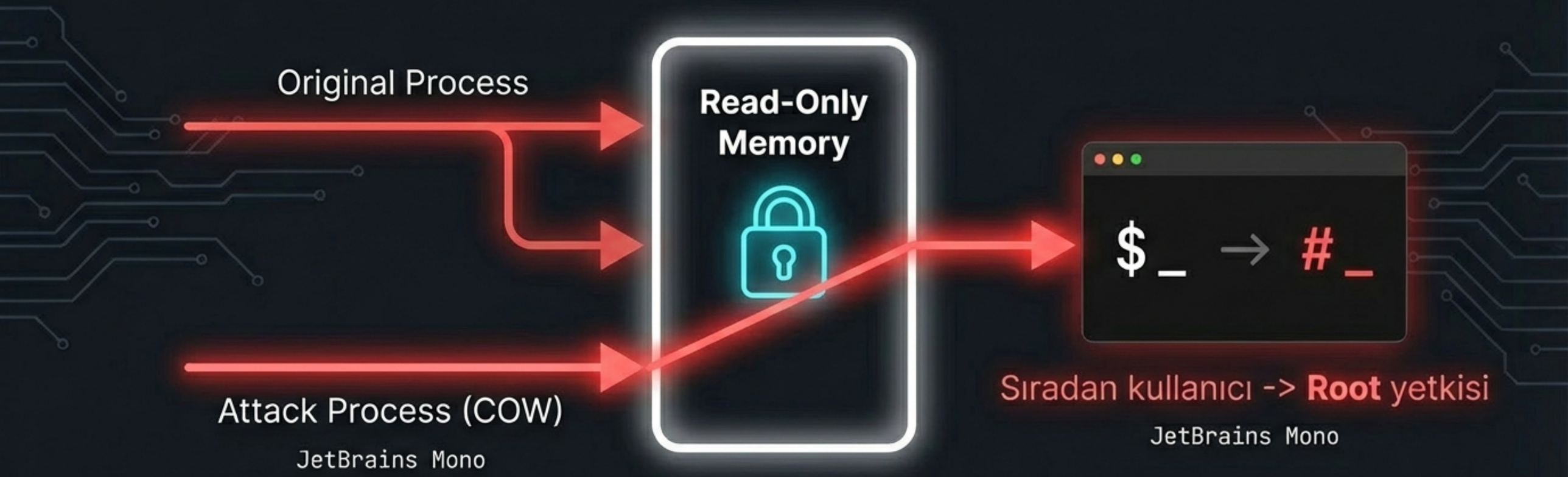
Sticky Bit

Genellikle **/tmp** dizininde. Sadece dosya sahibi silme işlemi yapabilir.

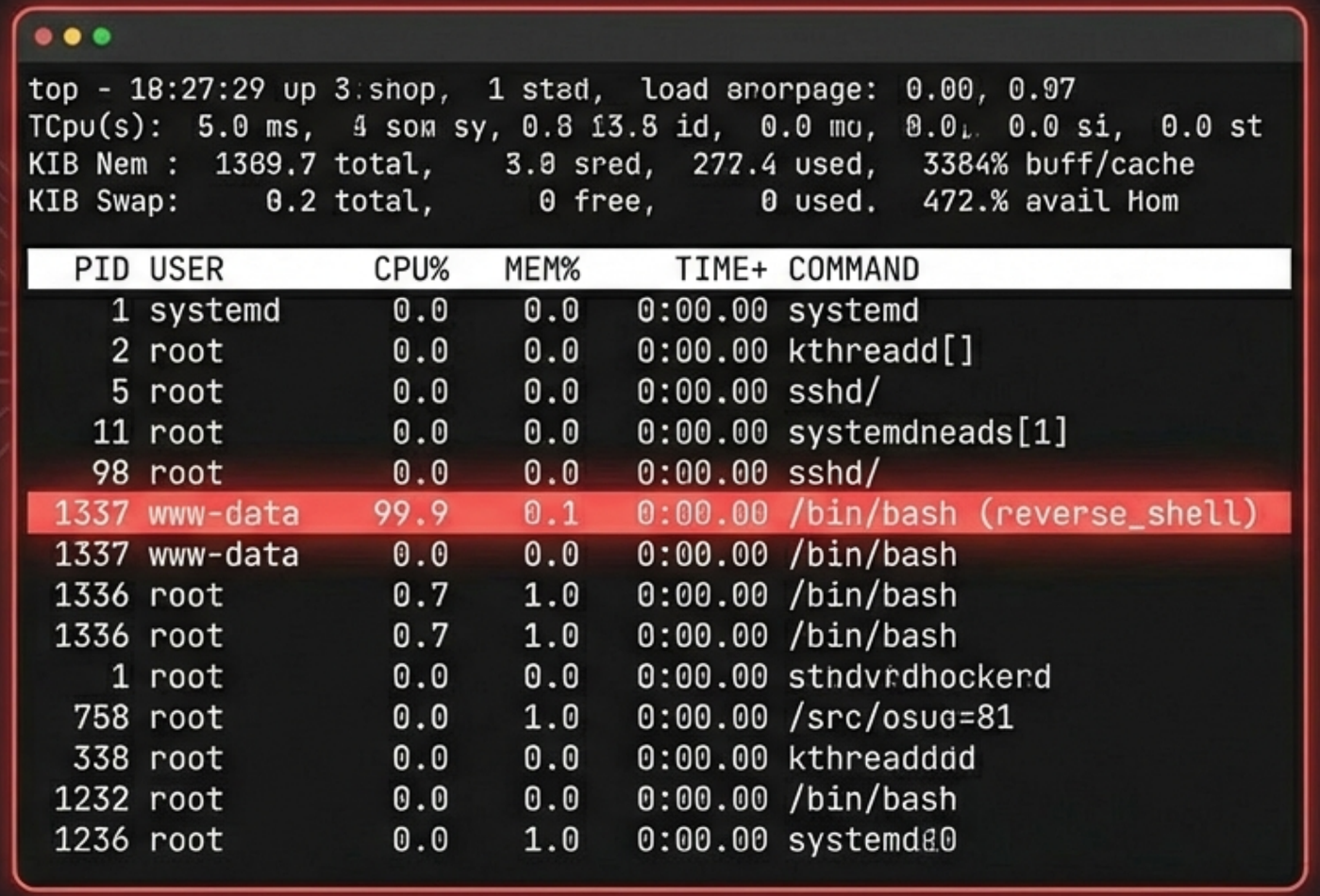
Kalp: Linux Çekirdeği (Kernel)

Kernel seviyesindeki zafiyet, tüm güvenlik katmanlarını aşar.

Kernel Exploit: Dirty COW (CVE-2016-5195)



Nabız: Proses Yönetimi



- Kimlik: PID & PPID
- Anomali: Web sunucusu shell (kabuk) başlattı.
- **Komutlar:** ps aux, top, kill

Surlar: OSI Modeli ve Saldırı Katmanları

SQL Injection, Phishing

JetBrains Mono

SYN Flood

IP Spoofing

ARP Spoofing

JetBrains Mono

Radar: Ağ Keşfi ve Dinleme

- **Active Recon (Nmap):** Kim orada? Port taraması ve versiyon tespiti.
- 🚨 **Passive Recon (Tcpdump):** Ne konuşuyorlar? Ağ trafiği ve paket analizi.

İzler: Log Analizi ve Olay Müdahalesi

Büyük Resim: Savunma Döngüsü

Güvenlik bir ürün değil, bir süreçtir.