

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 MİMARİSİ

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' *
```



```
int main() {
```

```
    if (process_id > 0) {
```

```
        // Initialize secure socket
```

```
        char *buffer = malloc(1024);
```

```
        while (data_available) {
```

```
            decrypt_data(buffer);
```

```
        }
```

```
        return 0;
```

```
    }
```

```
    if (process_id > 0) {
```

```
        // Initialize secure socket
```

```
        char *buffer = malloc(1024);
```

```
        while (data_available) {
```

```
            decrypt_data(buffer);
```

```
        }
```

```
        return 0;
```

```
    }
```

```
    if (process_id > 0) {
```

```
        // Initialize secure socket
```

```
        char *buffer = malloc(1024);
```

```
        while (data_available) {
```

```
            decrypt_data(buffer);
```

```
        }
```

```
        return 0;
```

```
    }
```

```
    if (process_id > 0) {
```

```
        // Initialize secure socket
```

```
        char *buffer = malloc(1024);
```

```
        while (data_available) {
```

```
            decrypt_data(buffer);
```

```
        }
```

**// AUDITABLE  
code section**

# 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

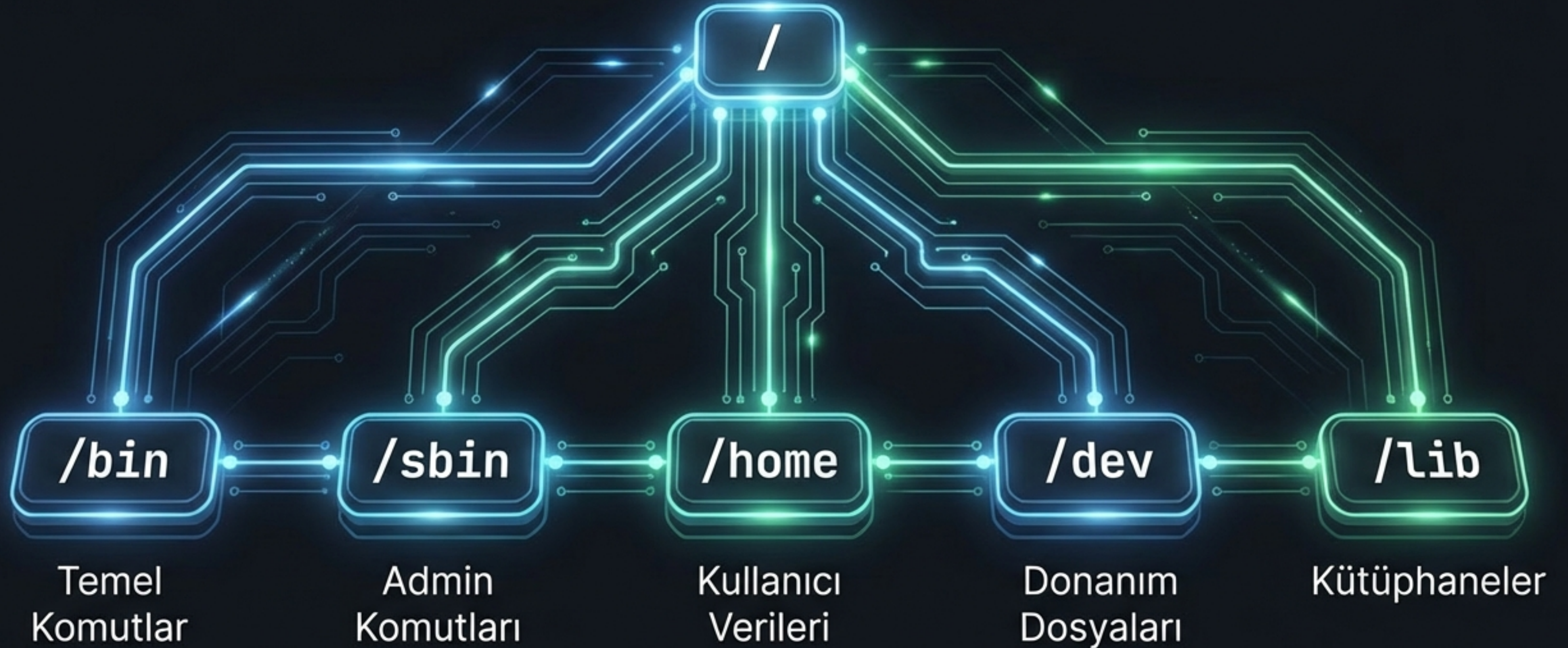
Savunma & Analiz

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



# Harita: Dosya Sistemi Hiyerarşisi (FHS)

Linux'ta her şey bir dosyadır.





# Kritik Bölgeler: Hedef ve Risk Noktaları

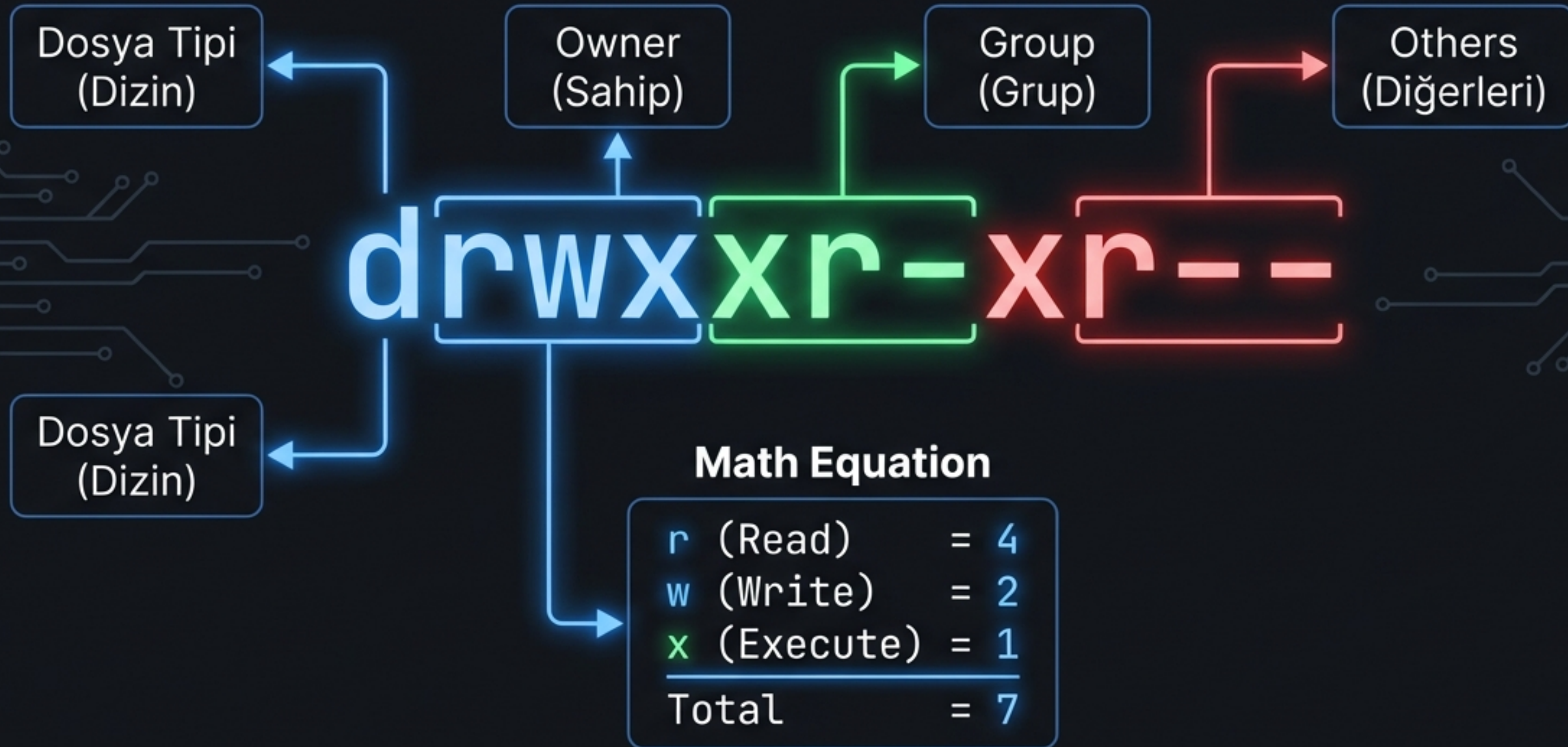
## Sinir Merkezi:

Konfigürasyon ve Kalıcılık Hedefi



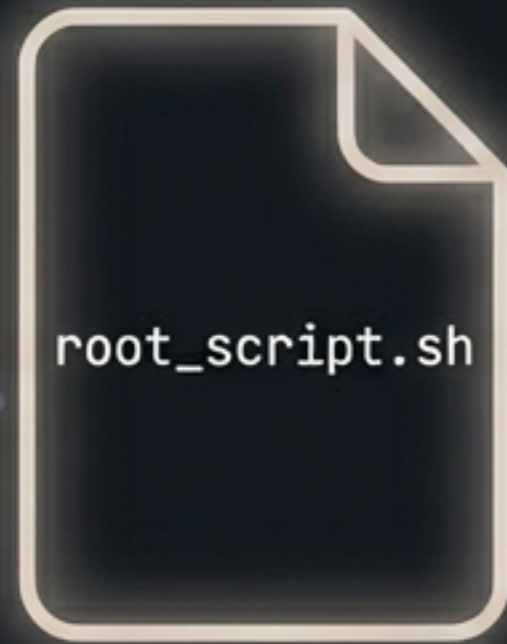


# Kapı Bekçileri: Dosya İzinleri





# Gizli Tehlikeler: Özel İzinler



-rw<sup>S</sup>r-xr-x

## SUID (SetUID)

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

## Sticky Bit

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



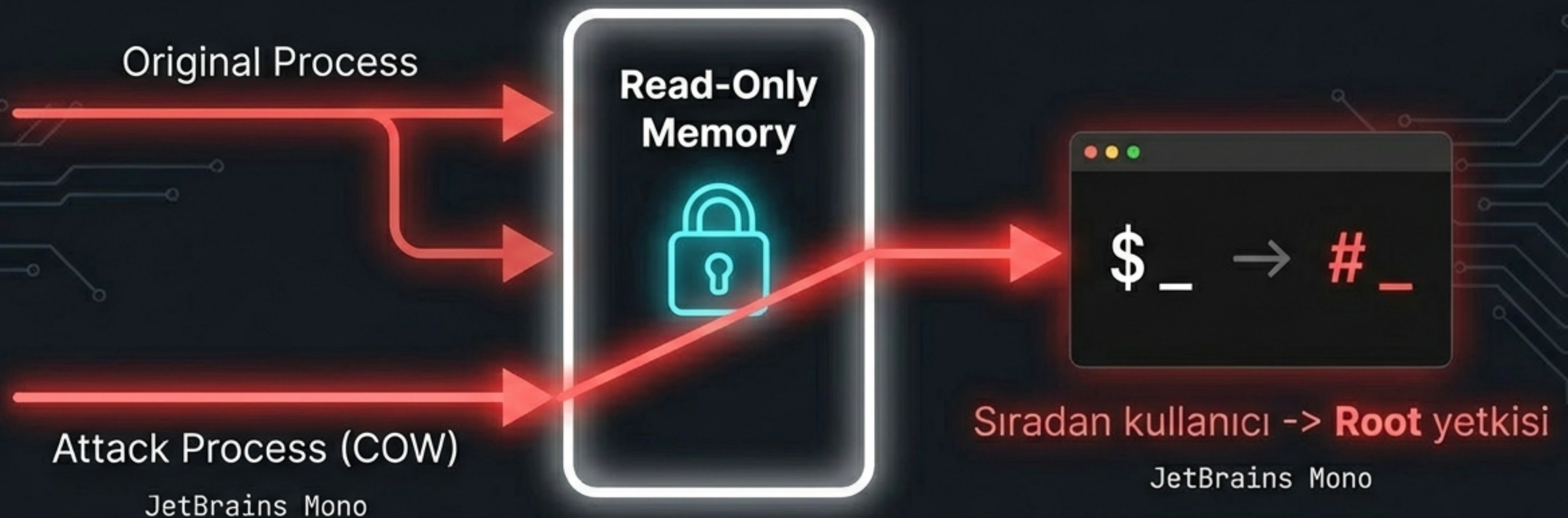
# Kalp: Linux Çekirdeği (Kernel)



Kernel seviyesindeki zafiyet, tüm güvenlik katmanlarını aşar.



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





# Nabız: Proses Yönetimi

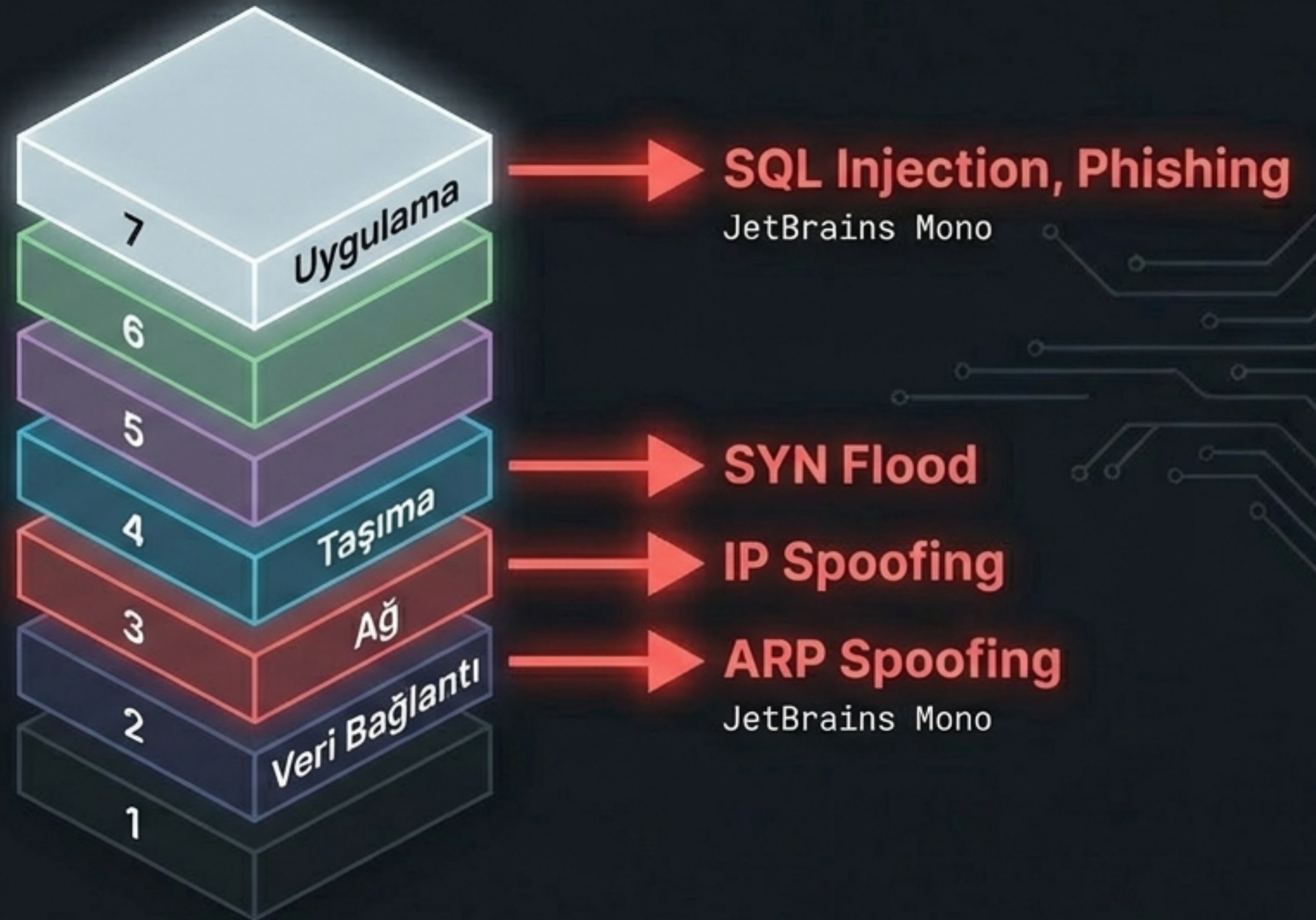
```
top - 18:27:29 up 3:shop, 1 stat, load average: 0.00, 0.07
TCpu(s):  5.0 ms,  4 sm sy, 0.8 id, 0.0 mn, 0.0 si, 0.0 st
KIB Mem : 1389.7 total,  3.0 sred, 272.4 used, 3384% buff/cache
KIB Swap:  0.2 total,  0 free,  0 used. 472.% avail Mem
```

| PID  | USER     | CPU% | MEM% | TIME+   | COMMAND                   |
|------|----------|------|------|---------|---------------------------|
| 1    | systemd  | 0.0  | 0.0  | 0:00.00 | systemd                   |
| 2    | root     | 0.0  | 0.0  | 0:00.00 | kthreadd[]                |
| 5    | root     | 0.0  | 0.0  | 0:00.00 | sshd/                     |
| 11   | root     | 0.0  | 0.0  | 0:00.00 | systemdneys[1]            |
| 98   | root     | 0.0  | 0.0  | 0:00.00 | sshd/                     |
| 1337 | www-data | 99.9 | 0.1  | 0:00.00 | /bin/bash (reverse_shell) |
| 1337 | www-data | 0.0  | 0.0  | 0:00.00 | /bin/bash                 |
| 1336 | root     | 0.7  | 1.0  | 0:00.00 | /bin/bash                 |
| 1336 | root     | 0.7  | 1.0  | 0:00.00 | /bin/bash                 |
| 1    | root     | 0.0  | 0.0  | 0:00.00 | stdvrdhockend             |
| 758  | root     | 0.0  | 1.0  | 0:00.00 | /src/osud=81              |
| 338  | root     | 0.0  | 0.0  | 0:00.00 | kthreadddd                |
| 1232 | root     | 0.0  | 0.0  | 0:00.00 | /bin/bash                 |
| 1236 | root     | 0.0  | 1.0  | 0:00.00 | systemd0                  |

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

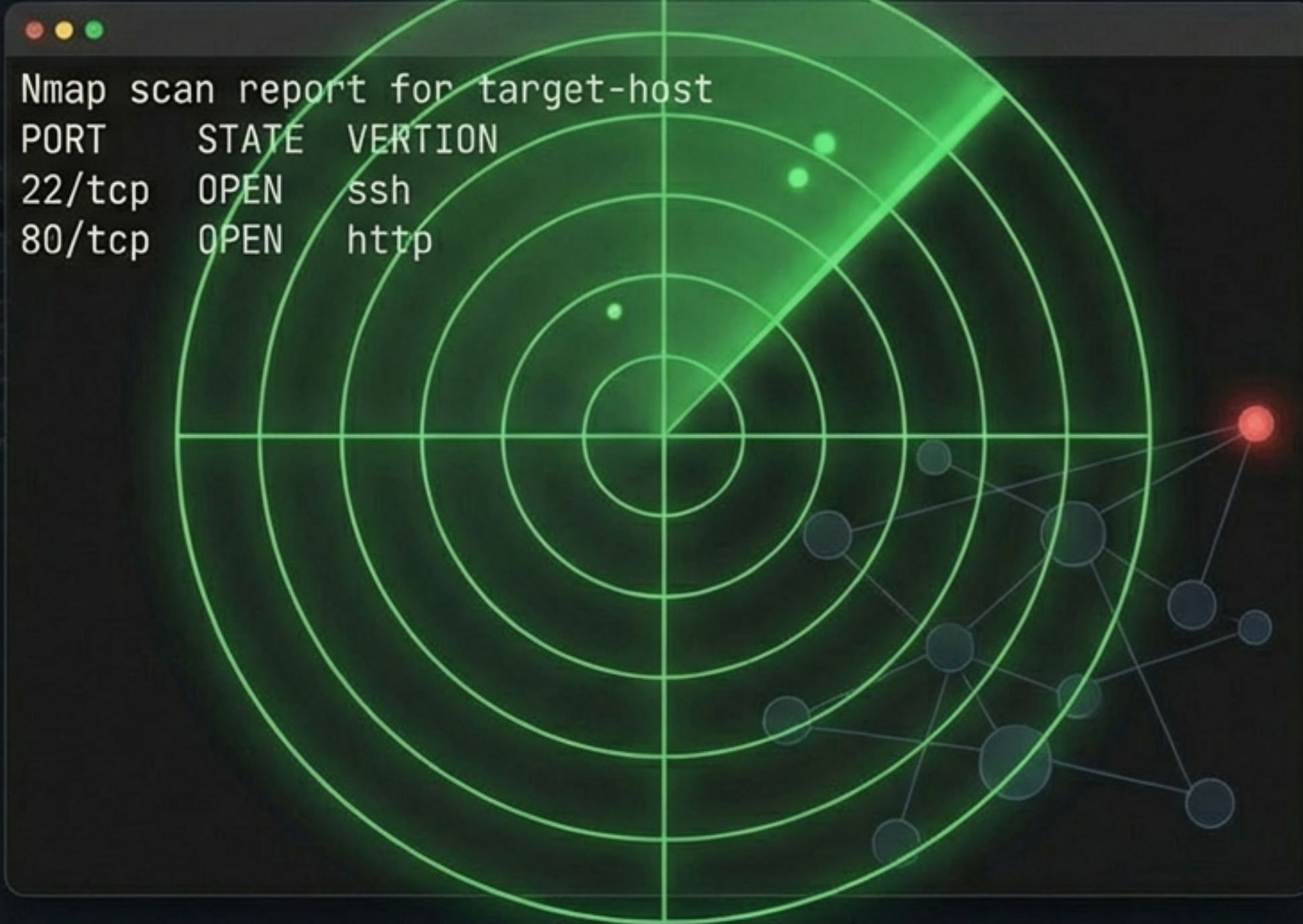


# Surlar: OSI Modeli ve Saldırı Katmanları





# 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

Hedef: /var/log/auth.log  
Araç: `grep 'Failed' /var/log/auth.log`



# Büyük Resim: Savunma Döngüsü



Güvenlik bir ürün değil, bir süreçtir.