Linux Dosya Sistemi ve Güvenlik Mimarisi

Hiyerarşi, İzinler ve Siber Güvenlik Analizi

DNA: Linux'ta Her Şey Bir Dosyadır

Donanım, süreçler ve soketler... hepsi dosya.

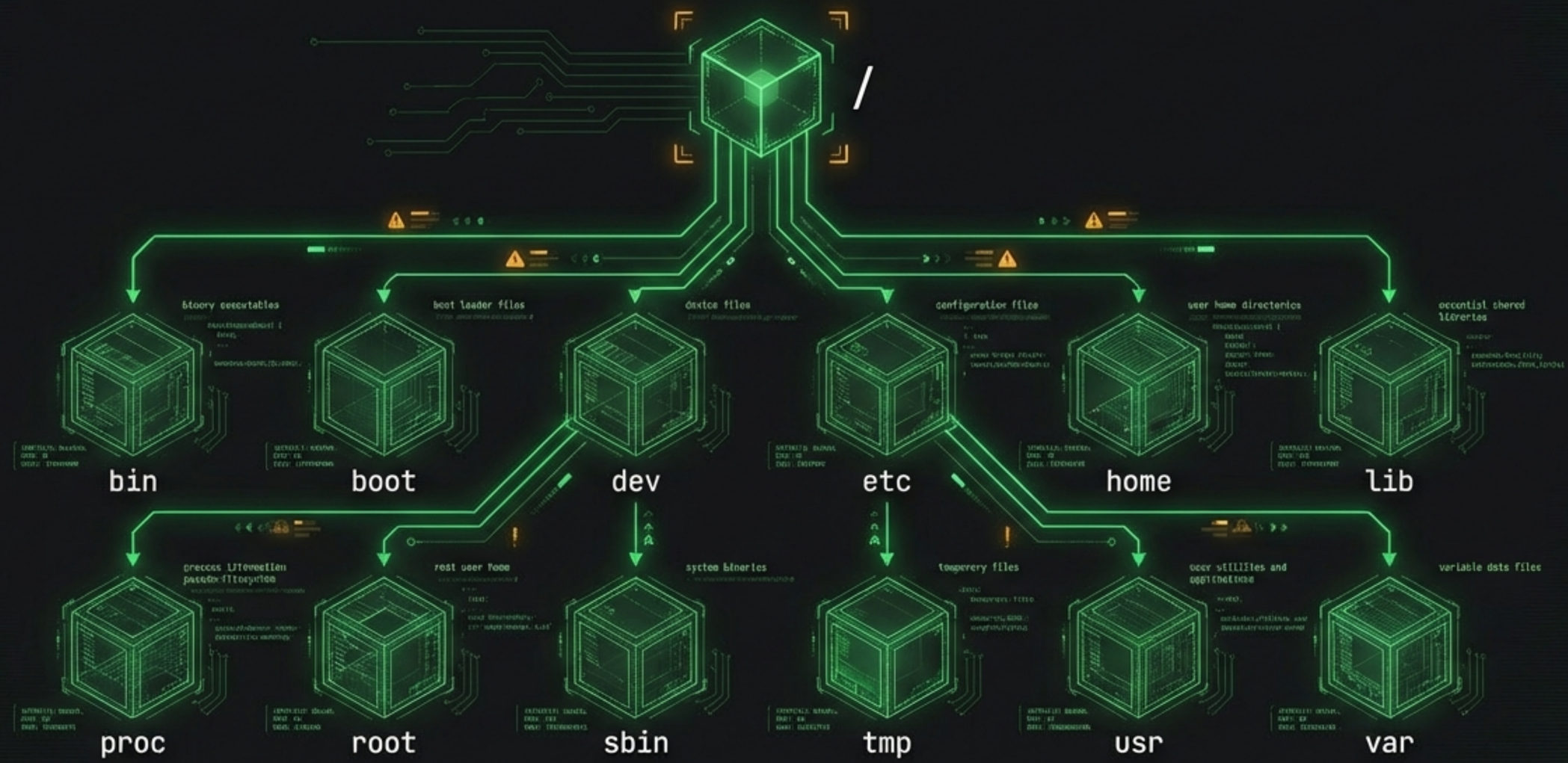
security insight

GÜVENLİK ANALİZİ

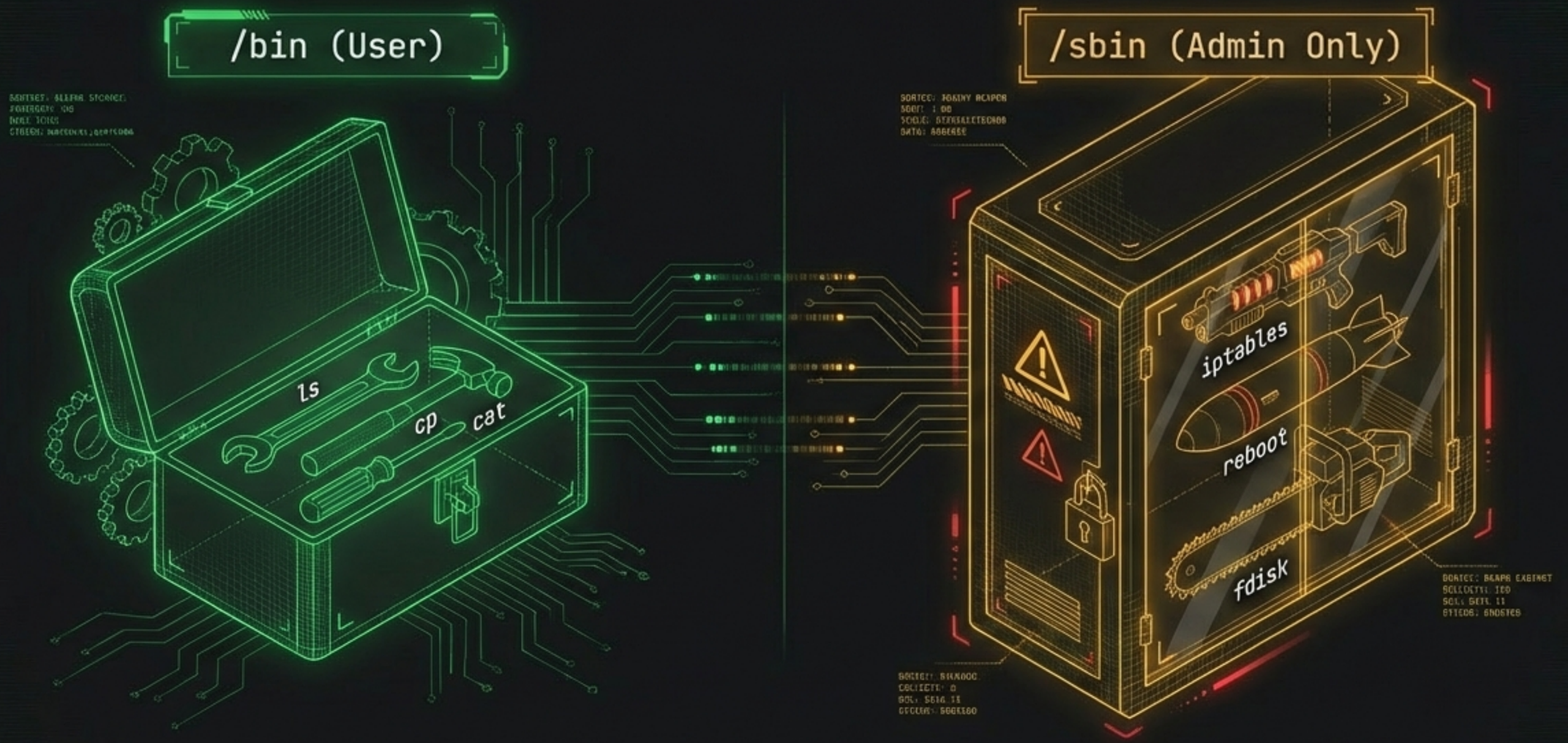
Bir dosyayı okuyup yazabiliyorsanız, o donanımı veya süreci **kontrol edebilirsiniz**.

Harita: Kök Dizin (The Root)

FHS (Filesystem Hierarchy Standard): Kaosu düzene sokan mimari plan.

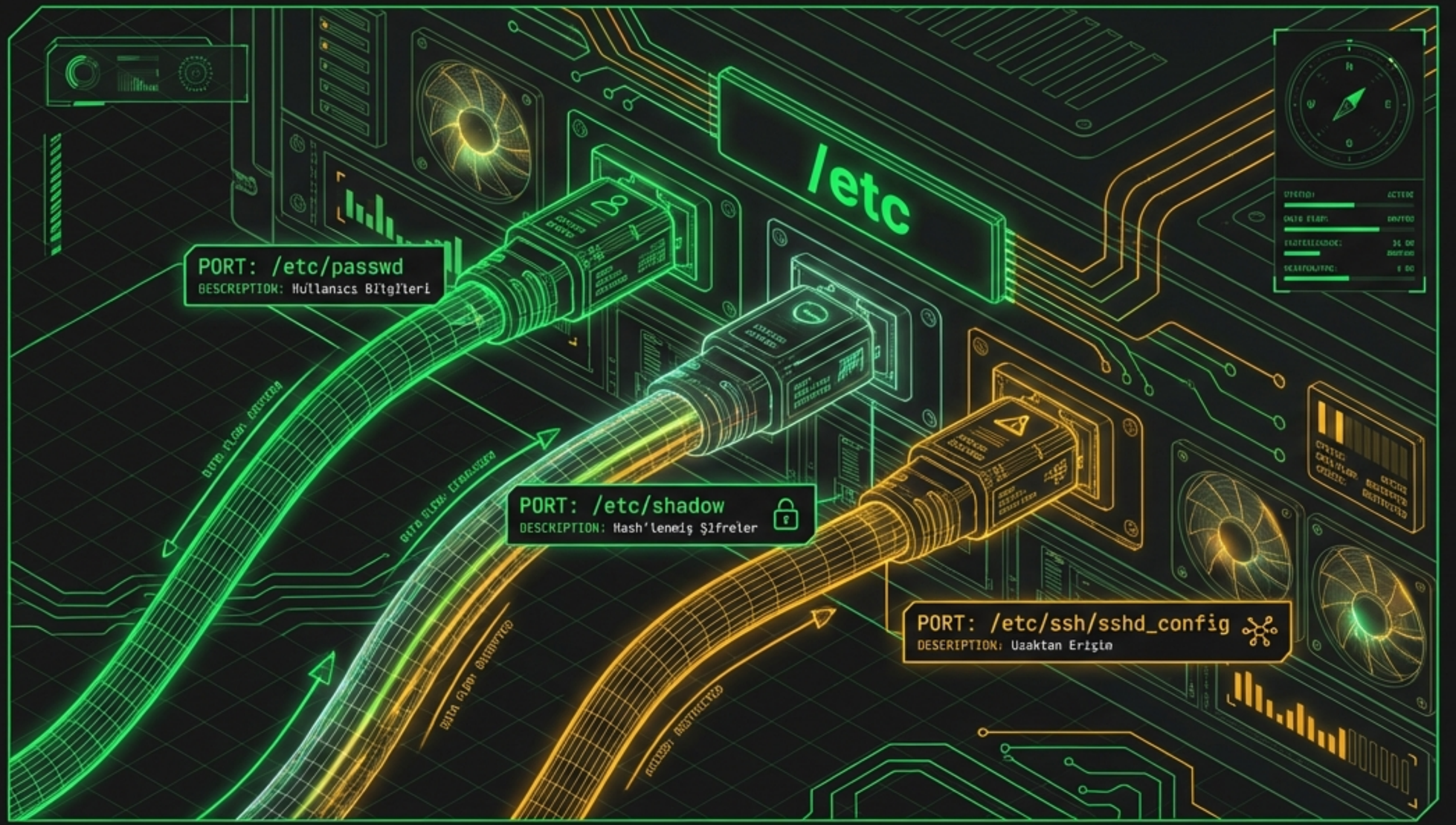


Araç Çantası: Binaries ve Kütüphaneler



Saldırganlar sistemde ilerlemek için bu araçları kullanır (Living off the land).

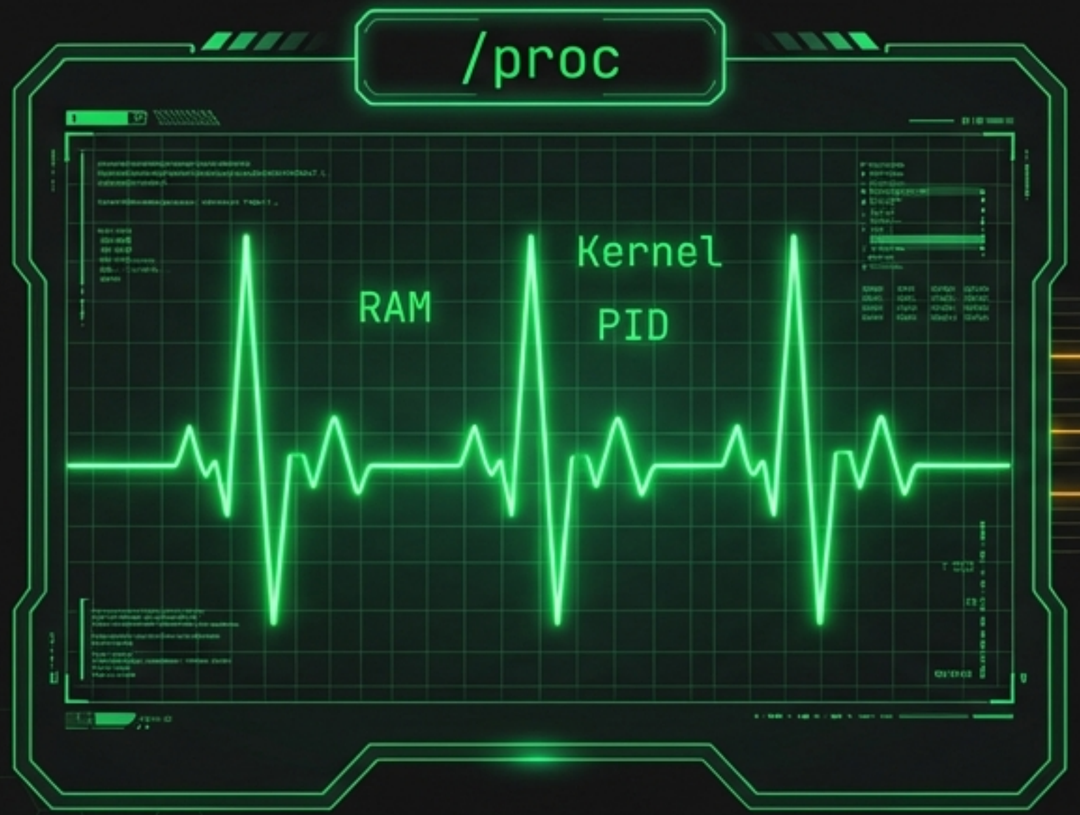
Beyin: Yapılandırma Merkezi (/etc)



Buradaki değişiklikler kalıcıdır. Persistence (kalıcılık) saldırıları burada gizlenir.

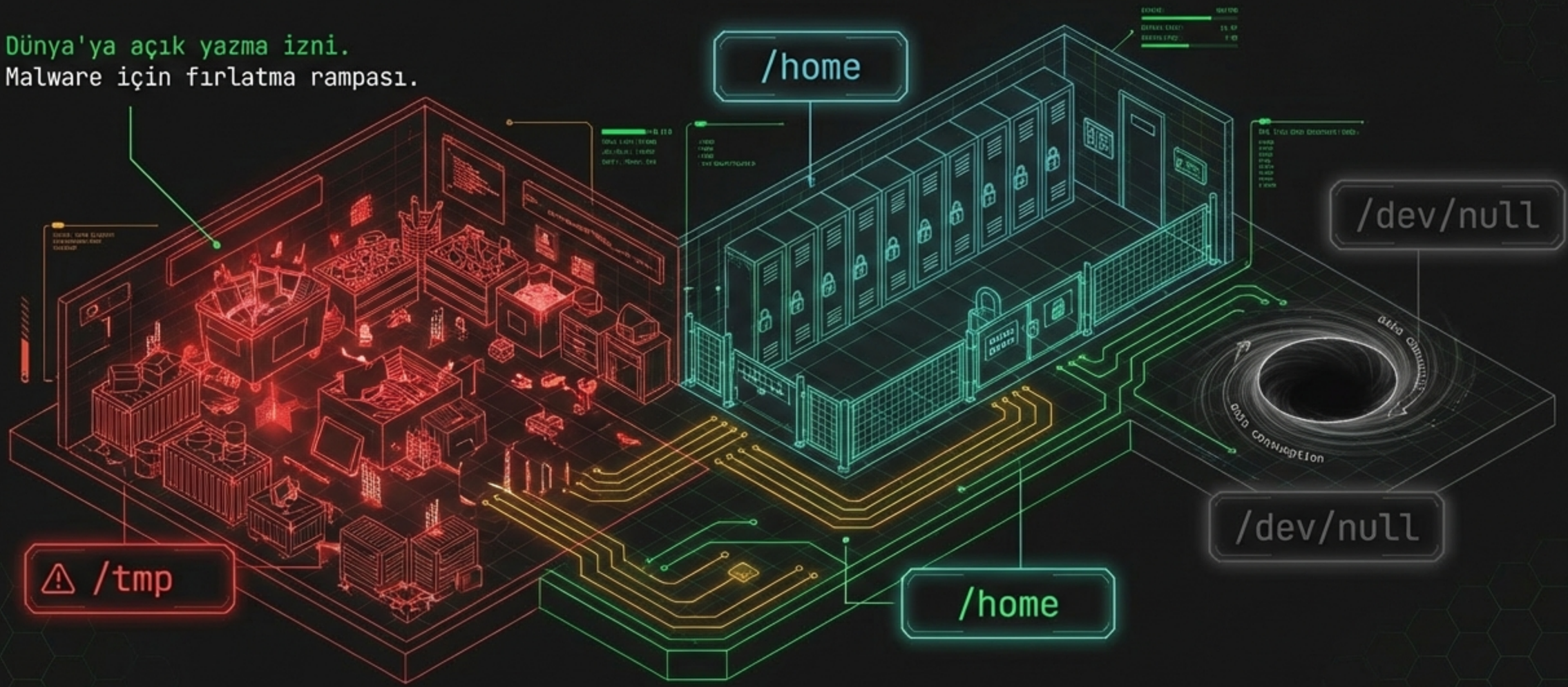
Nabız ve Kanıtlar: /proc ve /var

/proc: Anlık Analiz | /var: Adli Bilişim (Forensics)



Zafiyet Bölgeleri: /tmp, /home ve /dev

Dünya'ya açık yazma izni.
Malware için fırlatma rampası.



Güvenlik Bariyerleri: İzinler (RWX)

Read (r) = 4

Write (w) = 2

Execute (x) = 1

4 + 2 + 1 = 7 (Tam Yetki)

4 + 0 + 1 = 5 (Okuma & Çalıştırma)

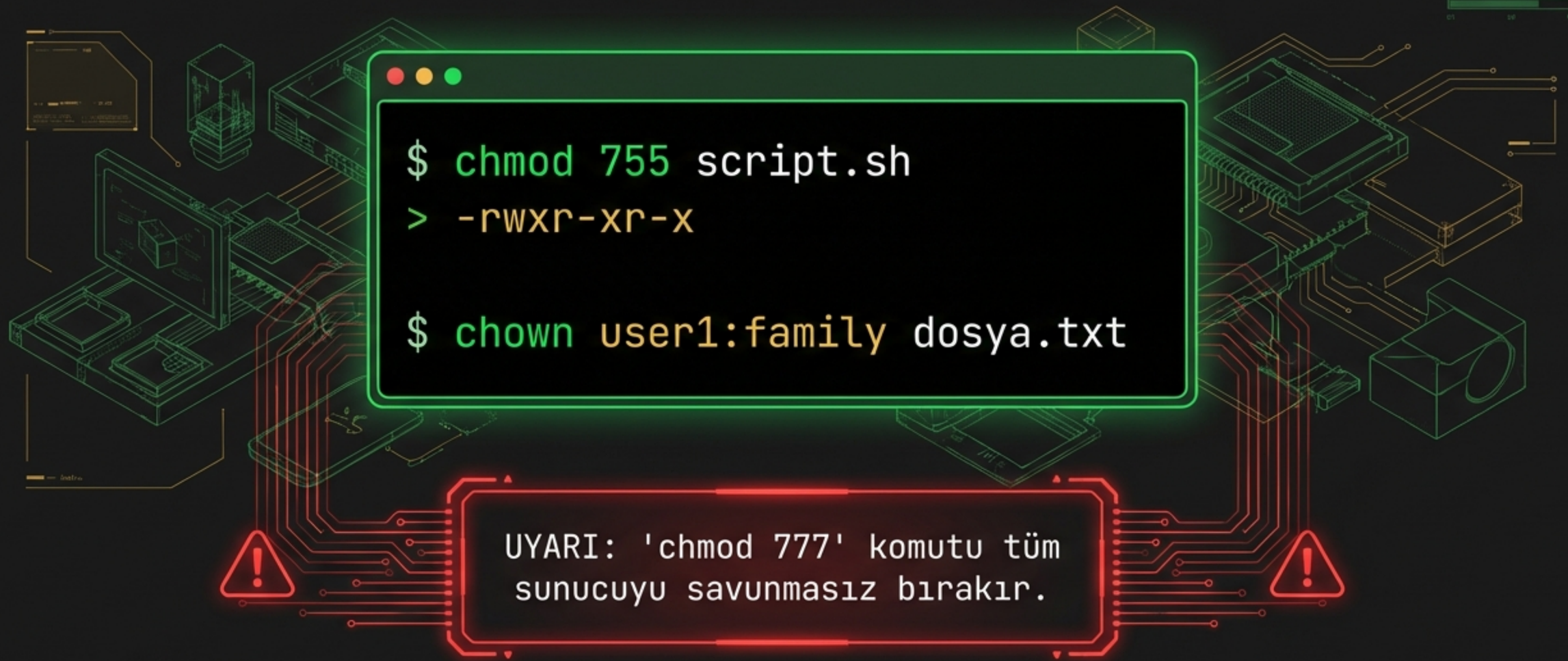
u (User/Owner)

g (Group)

o (Others)

Komuta Kontrol: chmod ve chown

Yönetici Komutları ve Sahiplik Değişimi



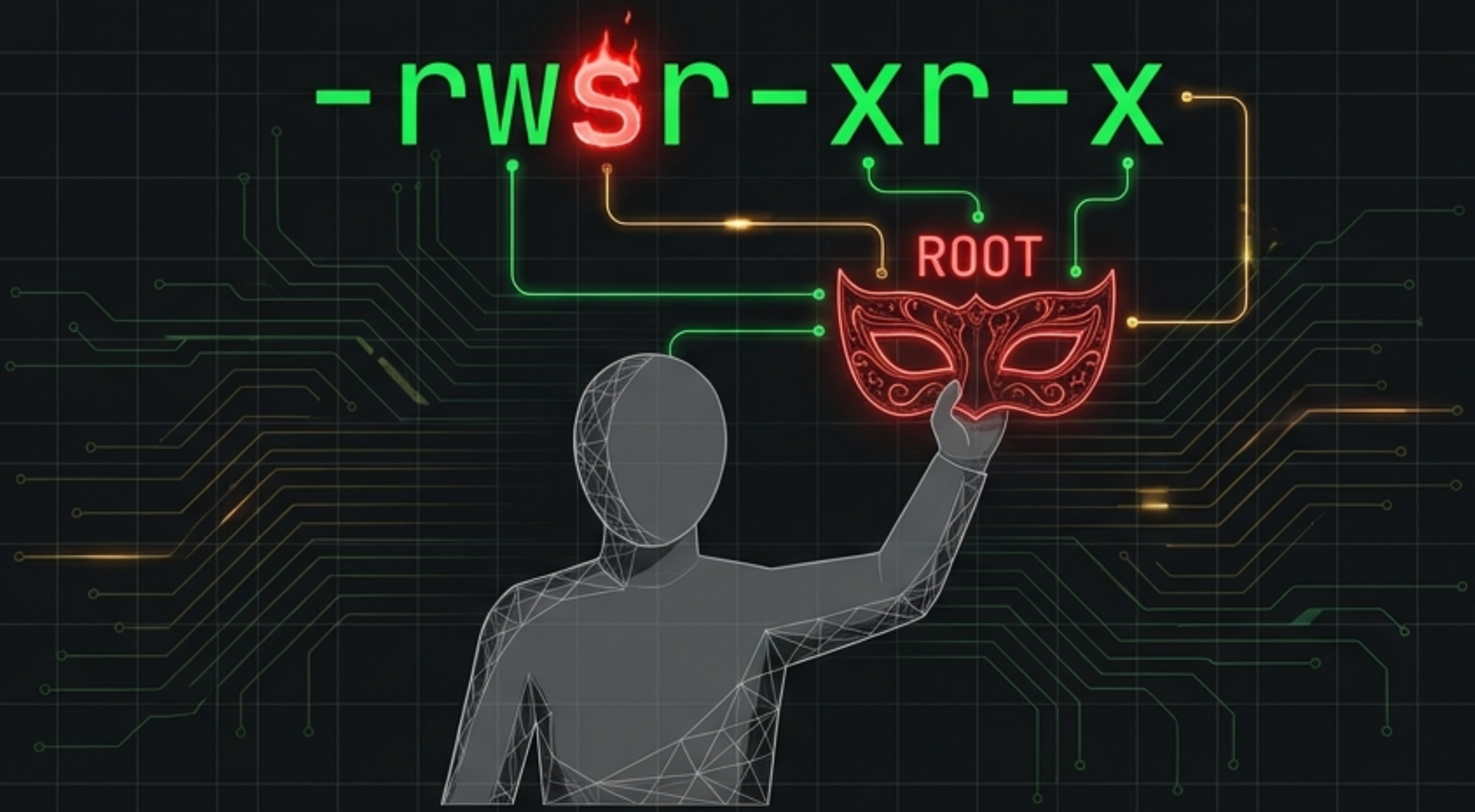
```
$ chmod 755 script.sh
> -rwxr-xr-x

$ chown user1:family dosya.txt
```

UYARI: 'chmod 777' komutu tüm sunucuyu savunmasız bırakır.

Gizli Geçitler: SUID ve SGID

Ödünç Alınan Güç. Dosya sahibi (Root) yetkisiyle çalışmak.



Cyber-Industrial Blueprint

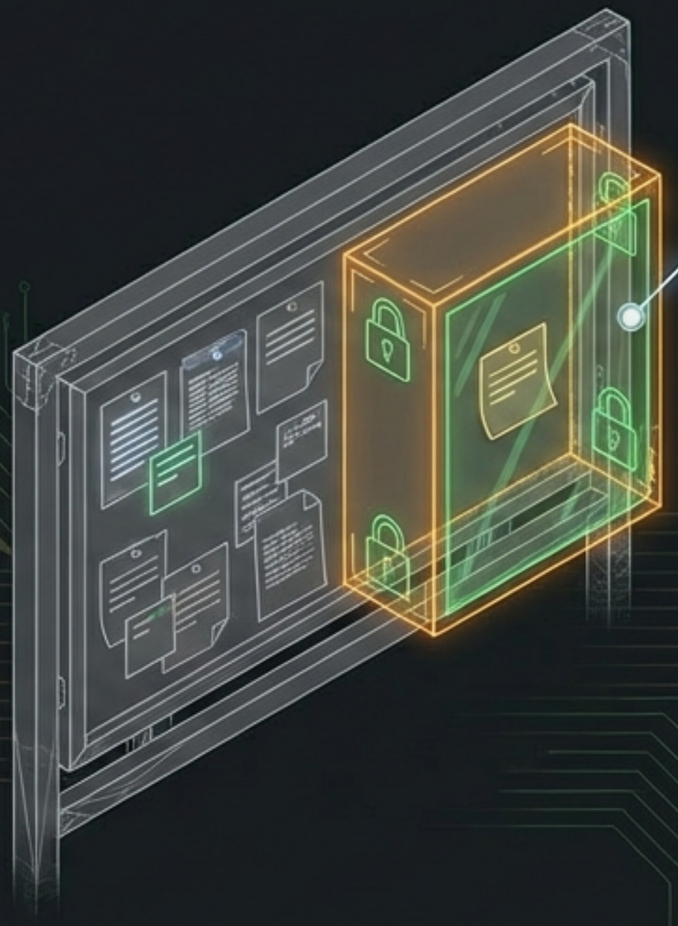
Saldırı Vektörü: Yetki Yükseltme

Privilege Escalation

Cyber-Industrial Blueprint

Karmaşayı Önlemek: Sticky Bit

/tmp güvenliği

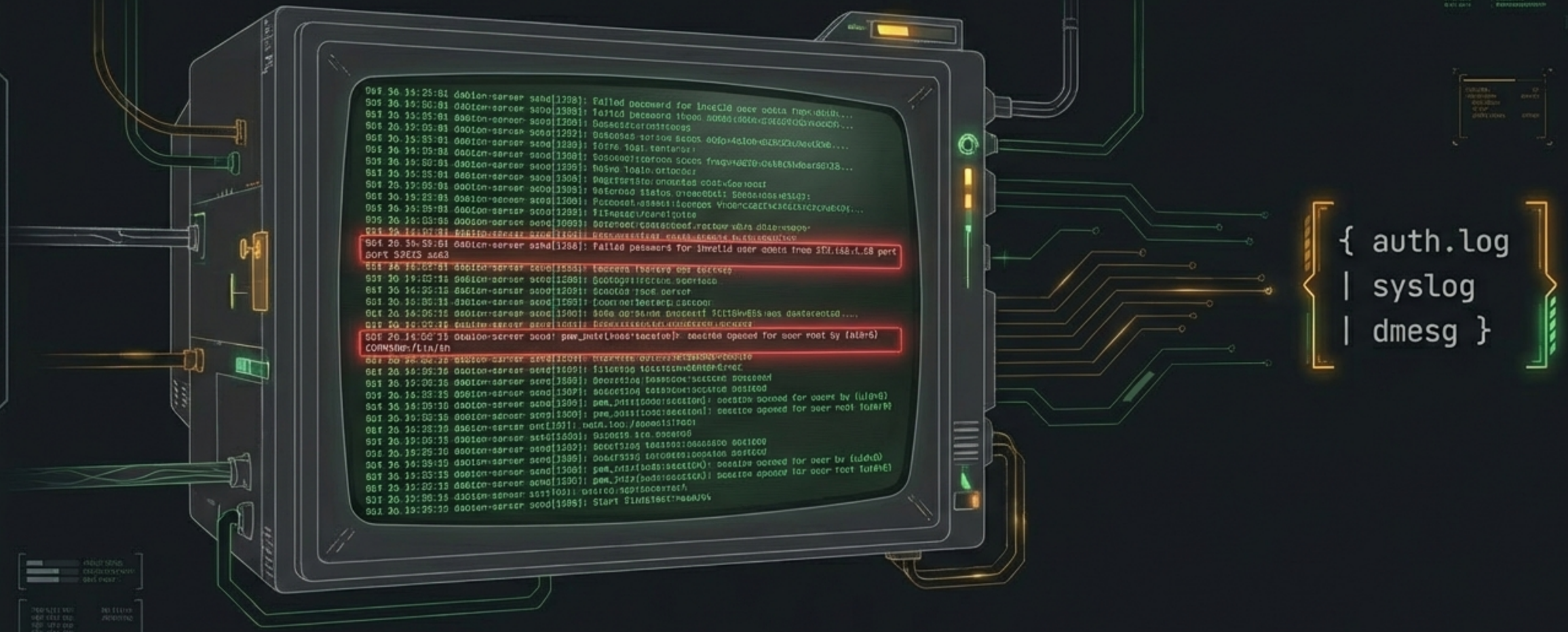


Sadece dosya sahibi silebilir. Diğerleri dokunamaz.

Cyber-Industrial Blueprint

Adli Bilişim: Log Analizi

/var/log



Cyber-Industrial Blueprint

Kaleyi Güçlendirmek: En İyi Uygulamalar

En Az Yetki Prensibi

SUID Dosyalarını Tara

/etc ve /var/log Kor Korumnası

/home Gizliliği (chmod 700) (chmod 700)

Sonuç

```
root@linux-fortress:~# _
```

Linux'ta her şey bir dosyadır. Dosyalarınızı korursanız, sistemi korursunuz.