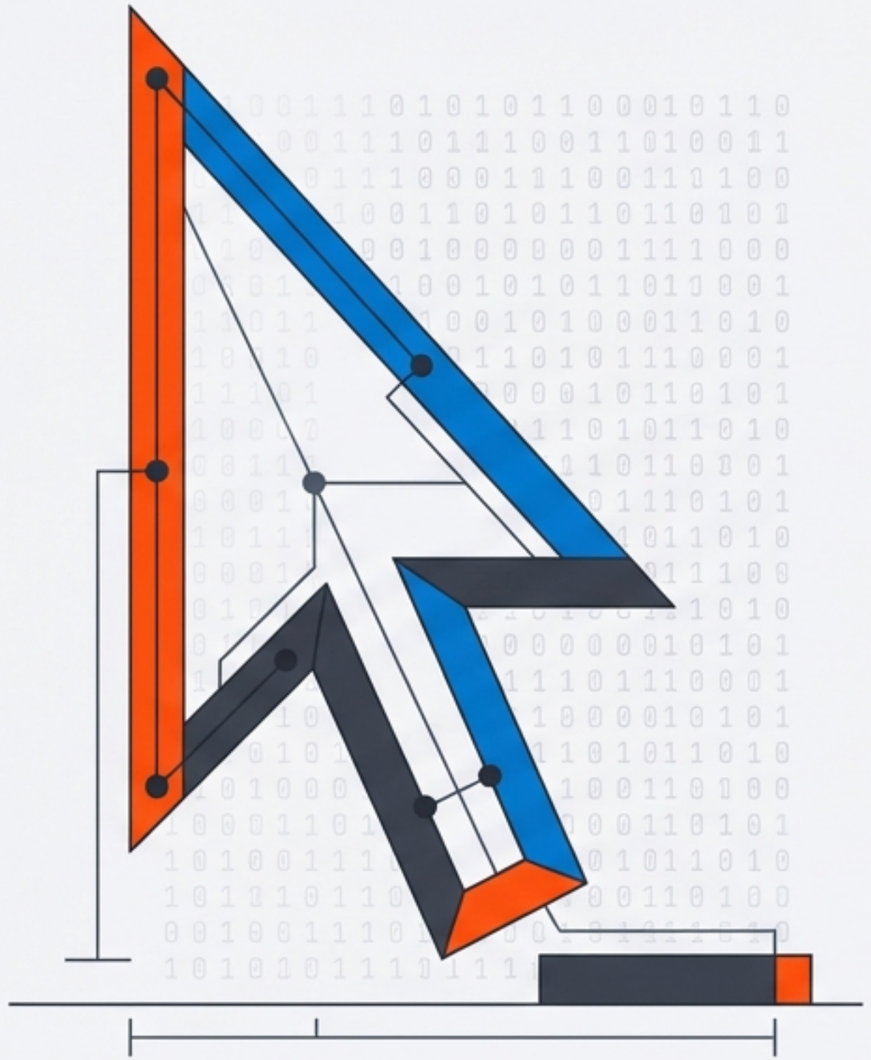
Linux Komut Satırı: Siber Güvenlik Uzmanının Nihai Silahı

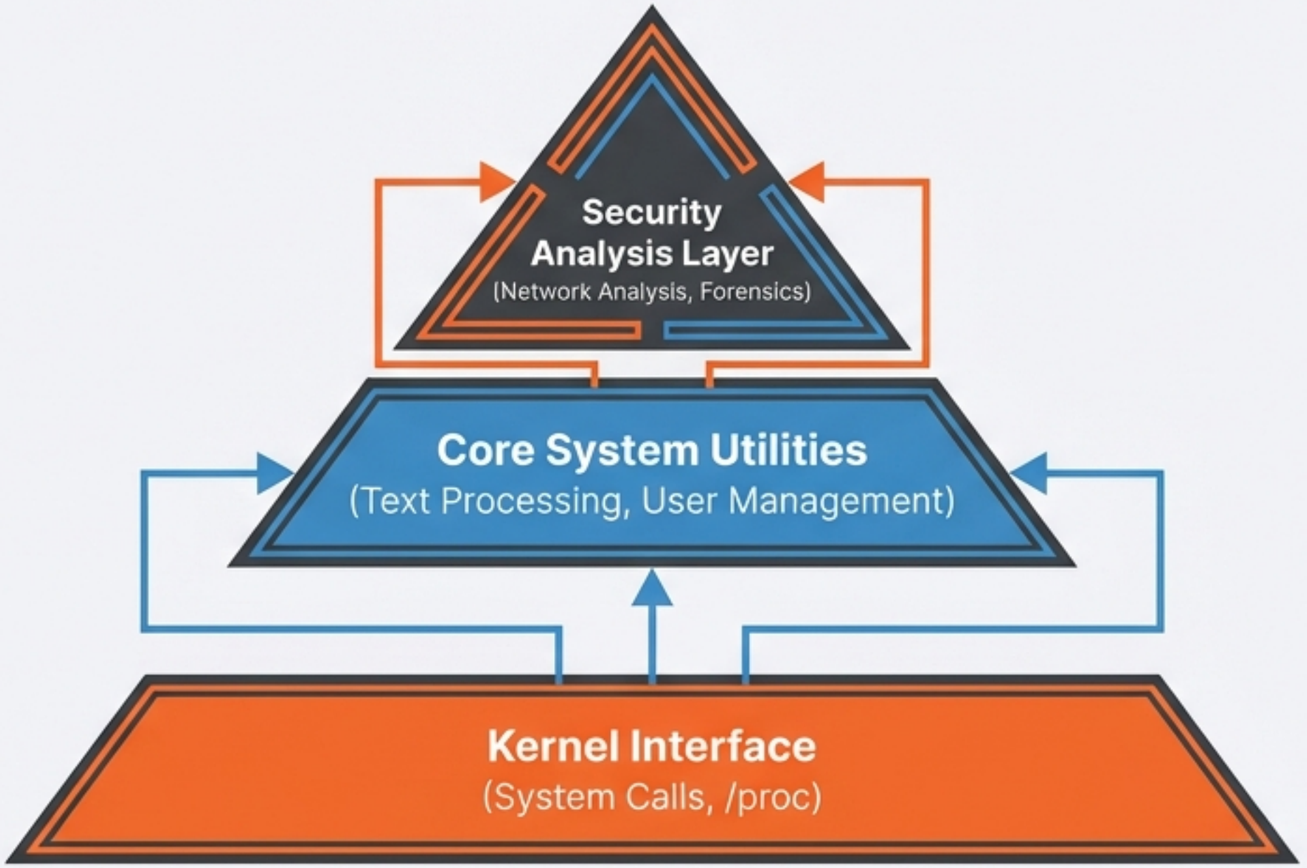
Operatörün Yolculuğu: Temelden Savunmaya

Grafik arayüzlerin bittiği yerde, gerçek kontrol başlar.



Neden Komut Satırı?

Grafik Arayüz (GUI) kolay işleri yapar. **Komut Satırı (CLI)** ise mümkün olmayan işleri yapar.



Görünürlük: Sistem çekirdeğine ve ham verilere doğrudan erişim.

Hız: Dakikalar süren işler, tek satır kodla saniyeler sürer.

Özgürlük: Tam kontrol ve bilme gücü.

Sahada Hakimiyet: Navigasyon ve Dosya Sistemi

Bir siber güvenlik olayı anında nerede olduğunuzu bilmek hayati önem taşır. Dosya sistemi bir labirenttir; haritayı okumayı öğrenin.

pwd

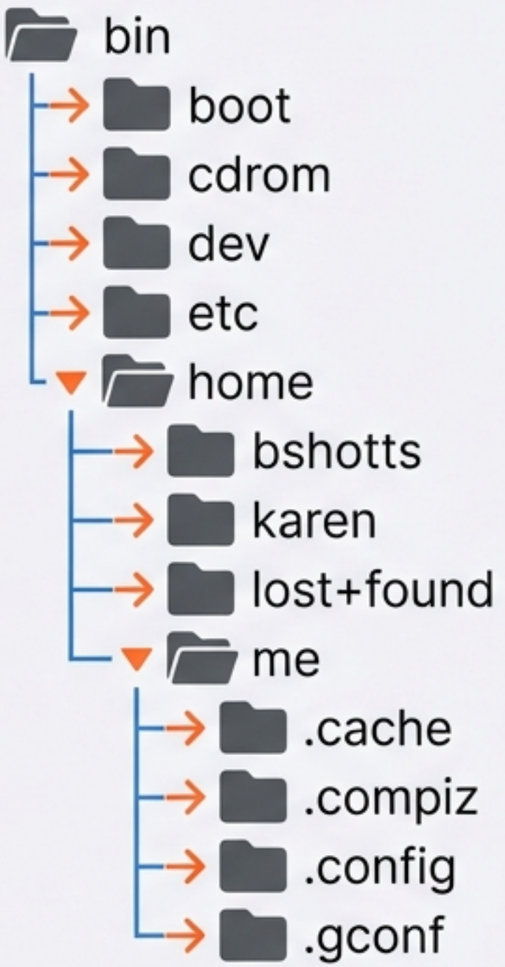
Neredeyim? (Mevcut çalışma dizini). Kaybolduğunuzda pusulanızdır.

`cd`

Işınlanma. Dosya ağacında hızla hareket etme.

`ls`

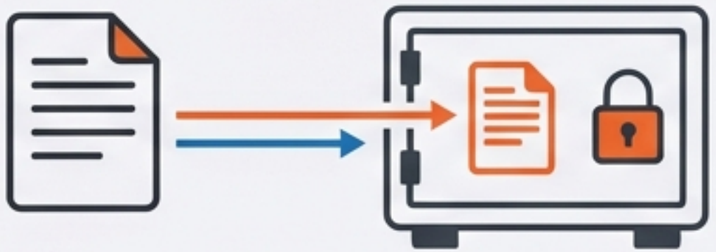
Keşif. Etrafınızdaki dosyaları ve dizinleri listeleme.



Dosya Manipülasyonu ve İzinler

“Her dosya bir hikaye anlatır. Dosyaya kimin erişebildiğini bilmek, hikayeyi çözmektir.”

Kanıt Toplama



`cp & mv` Kanıt dosyalarını güvenli bölgelere kopyalama veya taşıma.

Erişim Kontrolü

`chmod` Dosya izinlerini değiştirme (Örn: Zararlı yazılımı durdurmak).

`chown` Dosya sahipliğini değiştirme.

Pro Tip: `ls -l` çıktısındaki izinleri okumak, bir saldırganın sisteme arka kapı (backdoor) bırakıp bırakmadığını anlamanın ilk adımıdır.

Ağın Röntgesini Çekmek: ss ve netstat

Modern Linux dağıtımlarında `netstat` yerini daha hızlı ve detaylı olan `ss` komutuna bırakmıştır. Şüpheli bağlantıları tespit etmek için ilk durağımızdır.

```
[root@server ~]# ss -tnp
State    Recv-Q Send-Q Local Address:Port   Peer Address:Port   Process
ESTAB         0      0 192.168.1.5:22      10.0.0.89:53211     users:(("sshd",pid=1234,fd=3))
ESTAB         0      0 192.168.1.5:4444    198.51.100.1:80     users:(("bash",pid=9999,fd=3))
```

ESTABLISHED: Aktif veri alışverişi.

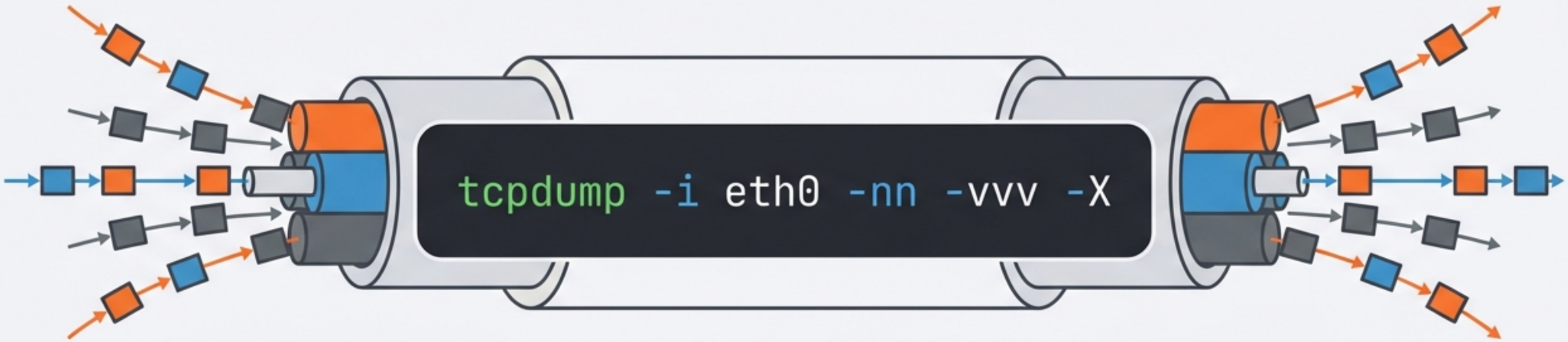
Bağlantı Uçları: Kiminle konuşuyoruz?

Process ID: Bağlantıyı başlatan uygulama.

Senaryo: Bilinmeyen bir dış IP adresine bağlı `bash` süreci görürseniz, sisteminizde bir 'Reverse Shell' olabilir.

Paket Seviyesinde Gerçekler: tcpdump

Ağ yalan söylemez, paketler konuşur.



Veri Sızdırma (DNS)

`tcpdump -i any -nn port 53` ile şüpheli DNS sorgularını ve tünellemeleri yakalayın.

HTTP Analizi

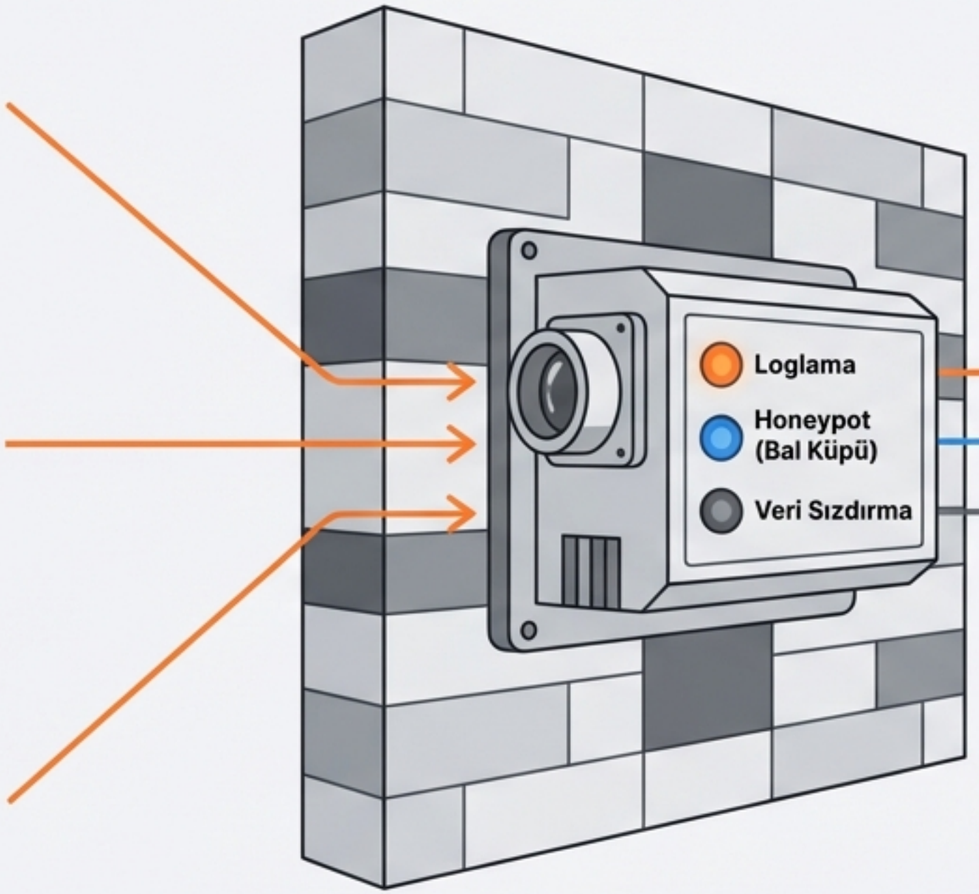
Şifrelenmemiş trafikteki kullanıcı adlarını veya zararlı istekleri `-A` bayrağı ile ASCII olarak görün.

ARP Spoofing

Yerel ağdaki 'Man-in-the-Middle' saldırılarını tespit edin.

Trafik Kontrolü ve Analizi: iptables

`iptables` sadece bir güvenlik duvarı değil, aynı zamanda güçlü bir analiz aracıdır.



1

Loglama

Saldırıları kaydetmek için LOG hedefini kullanın.

Terminal Block

```
iptables -I INPUT -j LOG --log-prefix "INPUT: "
```

2

Honeypot (Bal Küpü)

Kullanılmayan portlara (örn. Telnet - 23) gelen trafiği loglayarak saldırganı tespit edin.

3

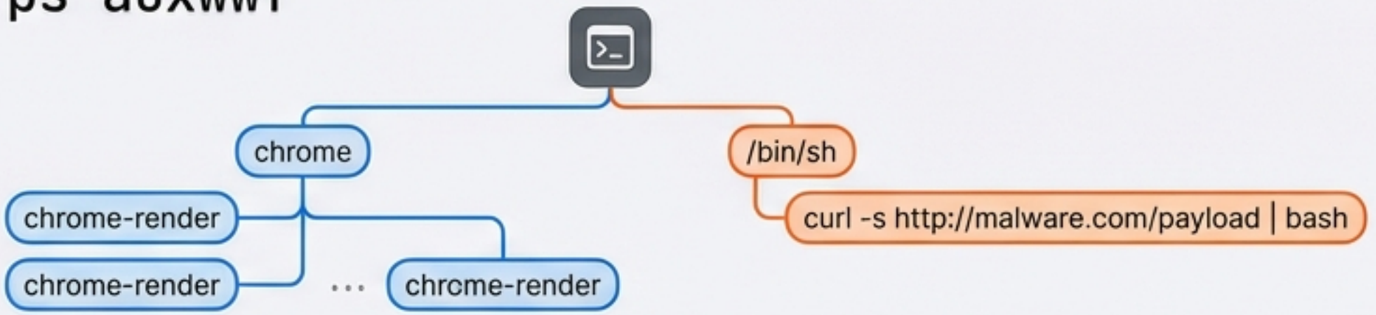
Veri Sızdırma

`OUTPUT` zincirini izleyerek dışarı giden yetkisiz trafiği yakalayın.

Süreç Dedektifliği: ps ve top

Zararlı yazılımlar genellikle masum isimlerin arkasına saklanır.

ps auxwwf




```
ps auxwwf
```

Süreçleri ağaç yapısında görün. Bir sürecin "ebeveyni" şüpheliyse, `ps` bunu ifşa eder.

top

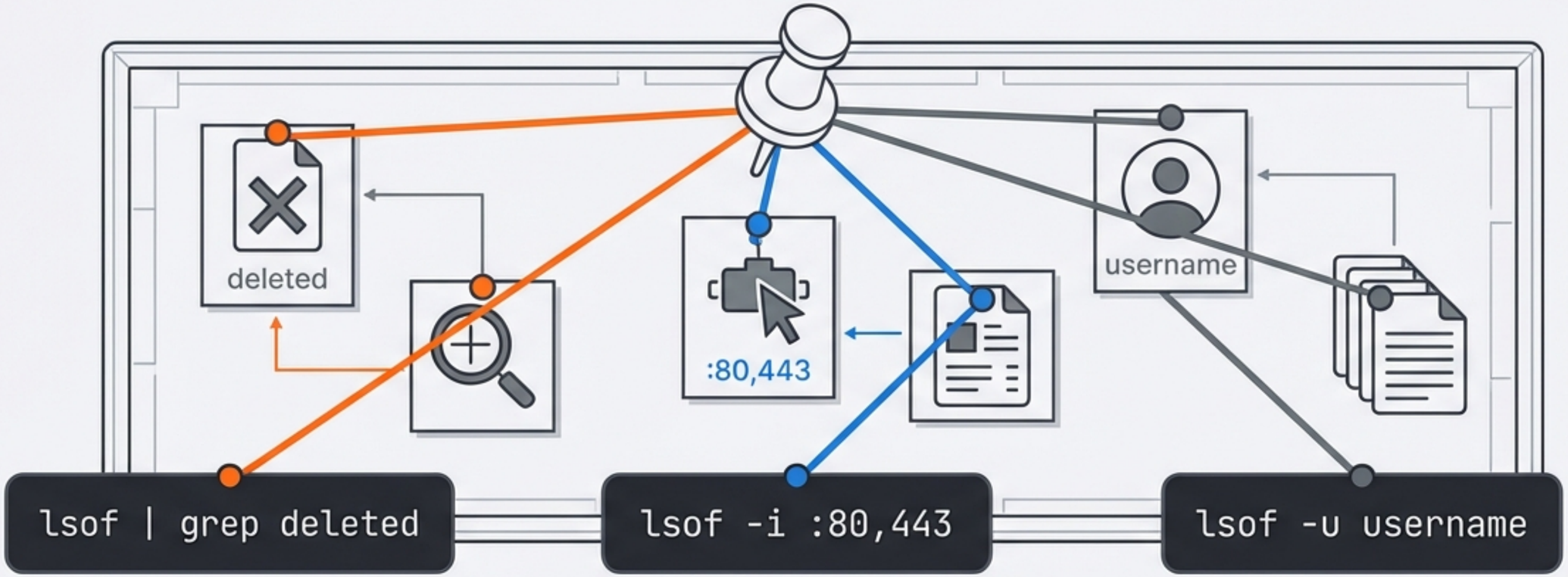

```
top - 10:45:00 up 2 days, 1 user, load average: 5.25, 3.10, 1.95

  PID USER   PR  NI  VIRT  RES   SHR S %CPU %MEM    TIME+ COMMAND
 4096 user   20   0  3.5g 512m  128m R 95.0  2.0 15:32.05 xmrig
```

Sistem yavaşladı mı? CPU kullanan Kripto Madencilerini (Crypto Miners) anlık olarak yakalayın.

Açık Dosyalar ve Soketler: lsof

Linux'ta "Her şey bir dosyadır". Ağ bağlantıları bile."



Disken silinmiş ama hafızada çalışan malware'i bulur.

Hangi dosyanın hangi portu kullandığını çözer.

Kullanıcının açtığı tüm dosyaları listeler.

Dosya Sistemi Adli Bilişimi: find

Bir olay sonrası analizde `find` komutu İsviçre çakısı gibidir.

Zaman Çizelgesi

```
find / -type f -mtime -1
```

Son 24 saatte değiştirilen dosyalar (Saldırgan ne yaptı?).

Gizli Dosyalar

```
find / -name ".*"
```

Nokta ile başlayan gizli dosyaları ortaya çıkarın.

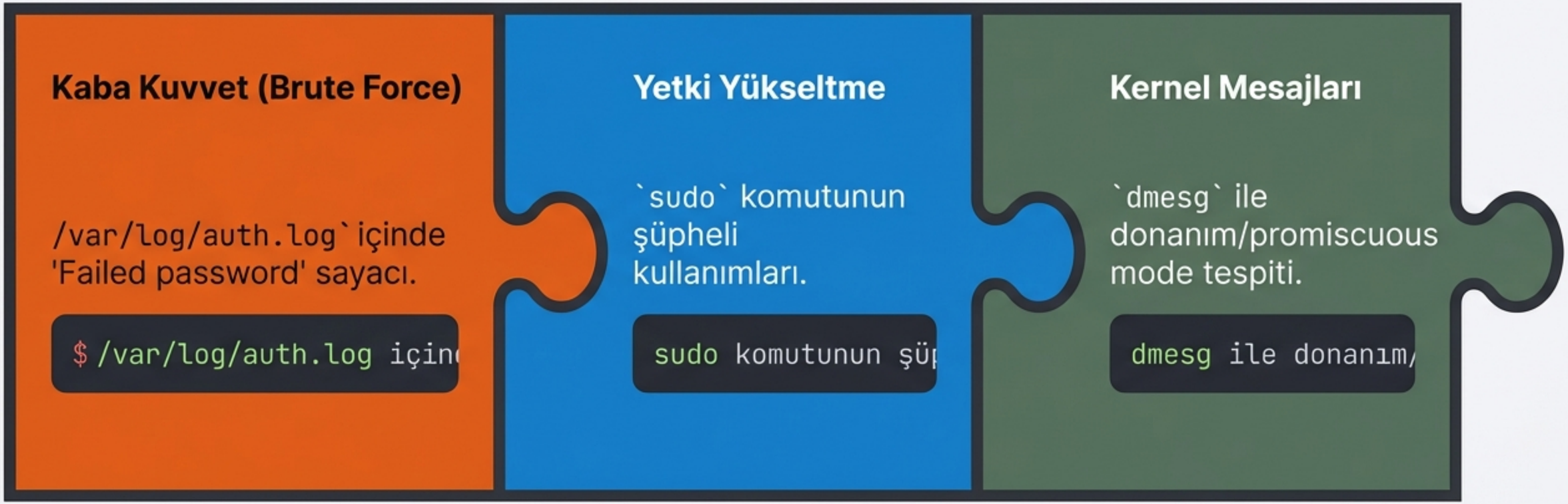
Risk Analizi

```
find / -perm -4000
```

Yetki yükseltme riski taşıyan SUID dosyalarını tespit edin.

Log Analizi ve Korelasyon

Farklı logları birleştirip büyük resmi görmek, saldırının anatomisini ortaya çıkarır.



Araçlar: `journalctl`, `grep`, `awk`.

Kullanıcı ve Erişim Denetimi

Sisteme kim, ne zaman ve nasıl girdi?

Oturum Takibi

```
last & w
```

komutları ile geçmiş ve anlık girişleri kontrol edin.

Gölge Hesaplar

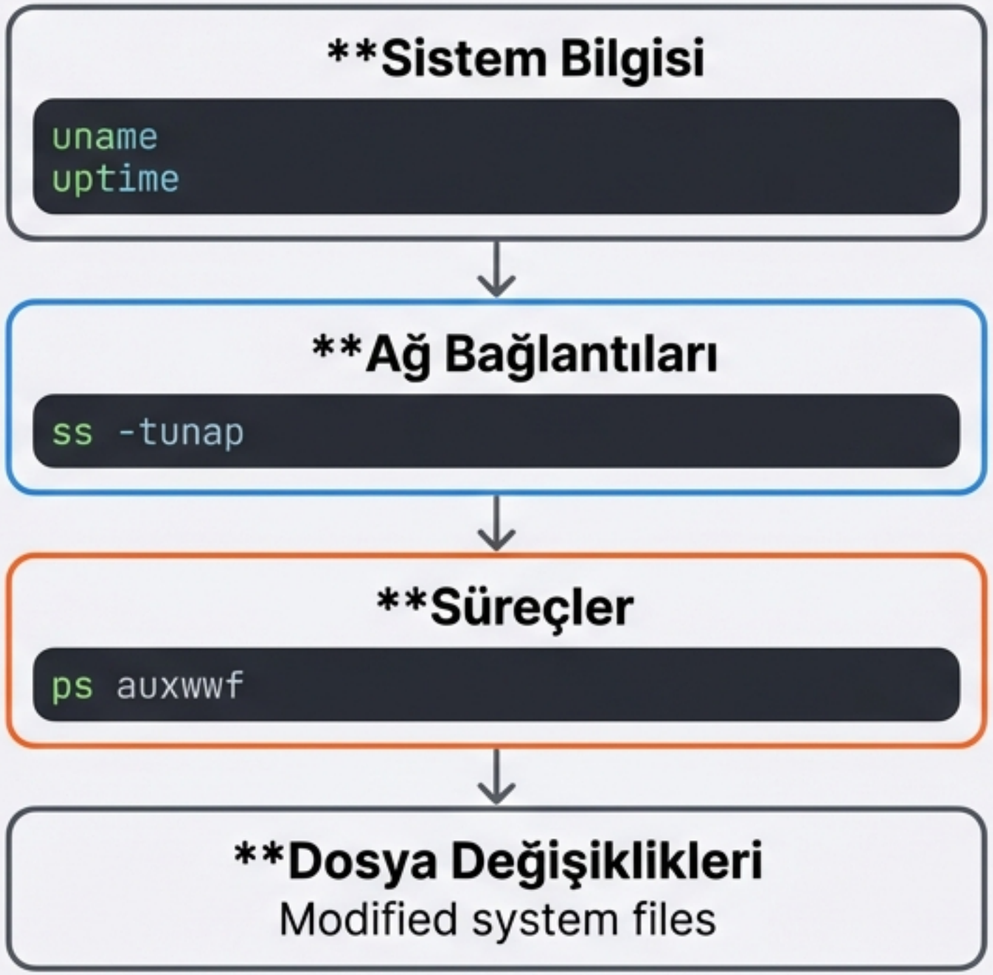
`/etc/passwd` dosyasında yetkisiz "hayalet" kullanıcıları (UID 0) arayın.

SSH Anahtarları

`authorized_keys` dosyalarında saldırganın bıraktığı anahtarları doğrulayın.

Olay Müdahale Akışı (Incident Response Triage)

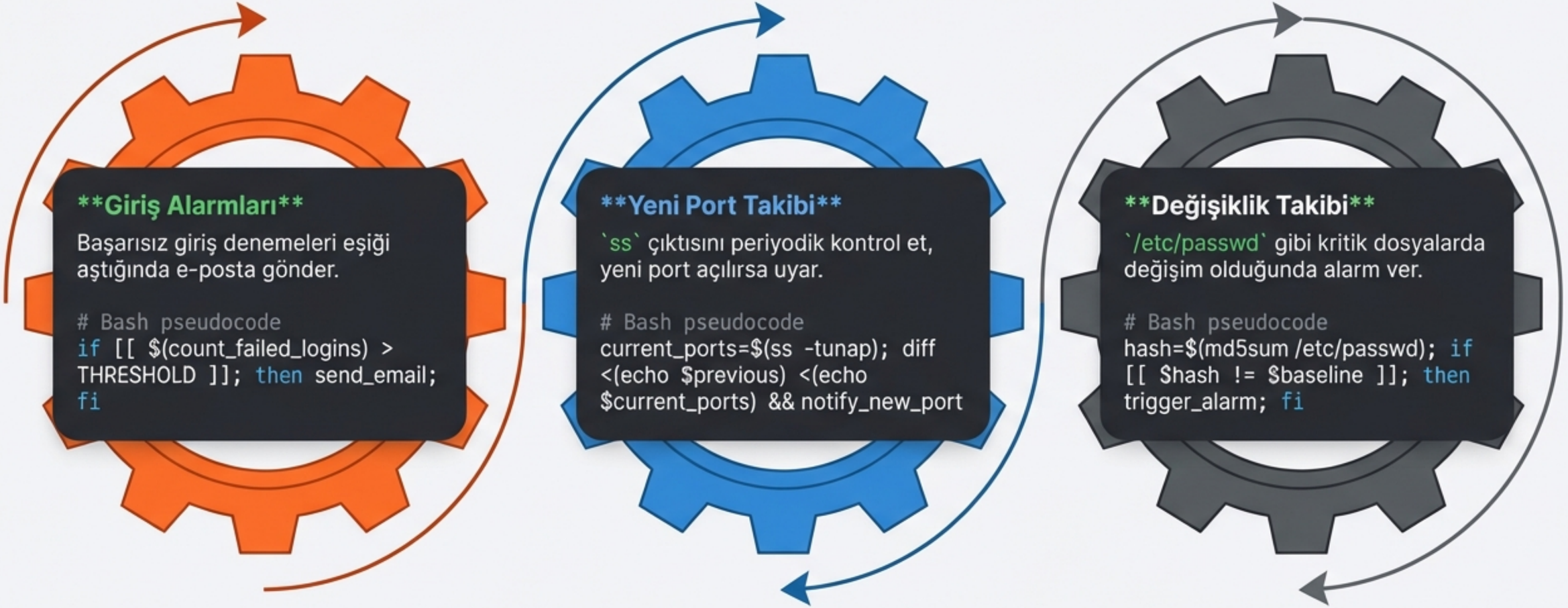
Bir saldırı anında panik en büyük düşmandır. Yapılandırılmış bir akış izleyin.



Hedef: Bu adımları bir betik (script) haline getirip, olay anında tek komutla "fotoğrafı çekmek".

Güvenlik Otomasyonu: Bash Scripting

Manuel kontrolleri otomatize edilmiş “sürekli izleme” betiklerine dönüştürün.



Sonuç ve En İyi Uygulamalar

Komut satırı sadece bir araç değil, siber savunmada en güçlü müttefikinizdir.

- **Kayıt Tutma (Logging):** Yaptığınız her işlemi loglayın (history, script logs).
- **Kaynak Yönetimi:** `top` ve `htop` ile sistemi yormadan analiz yapın.
- **Sürekli Öğrenme:** Tehditler evrildikçe, komut setinizi geliştirin.

Gerçek uzmanlık, sözdizimini (syntax) ezberlemek değil, sistemin nasıl çalıştığını anlamaktır.