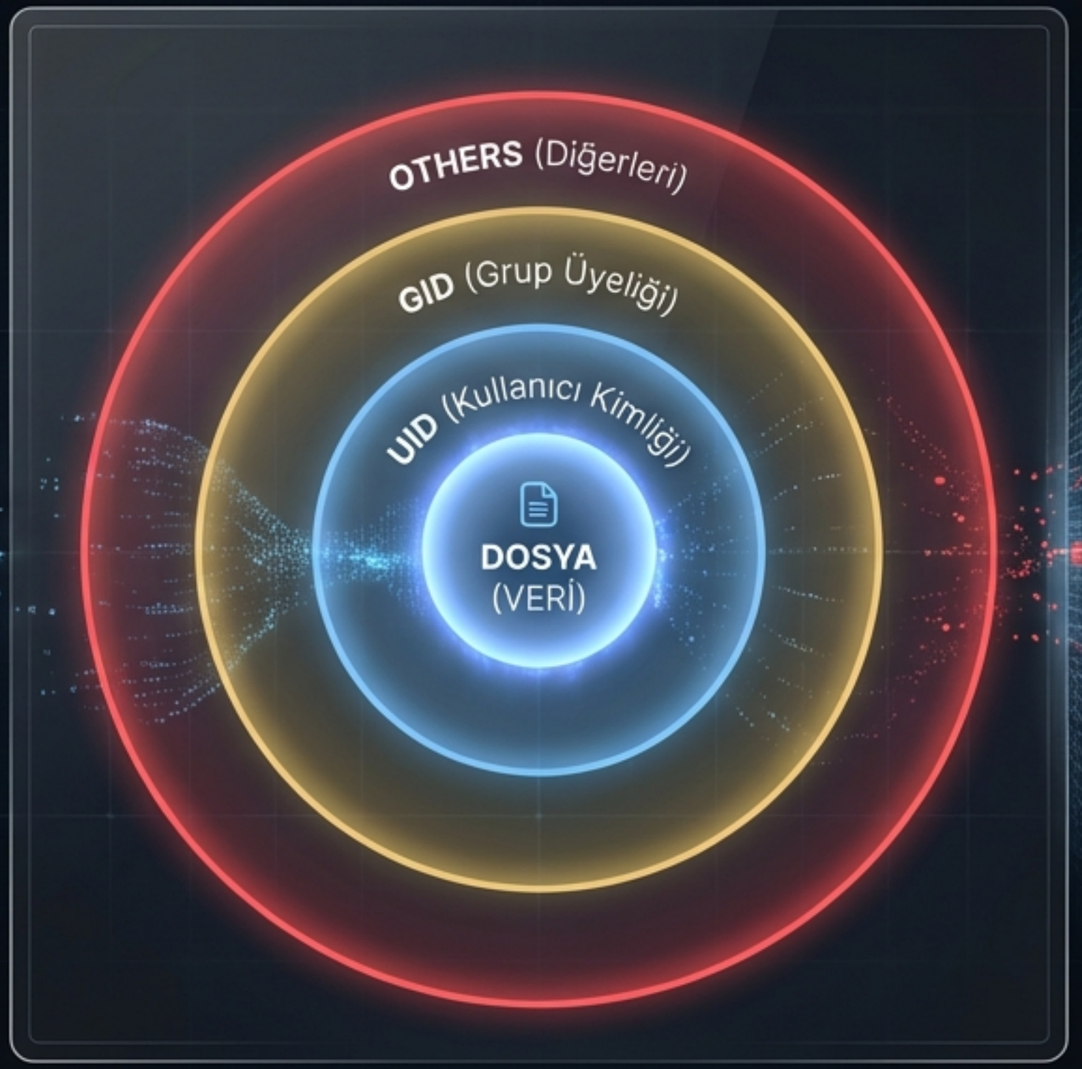
Linux Dosya Sistemi Güvenliği

Kullanıcılar, Gruplar ve İzinler


```
> init_security_protocol.sh
> Loading modules...
> Target: System Hardening
```

Kimlik Yönetiminden Yetki Yükseltme Risklerine Derinlemesine Bakış

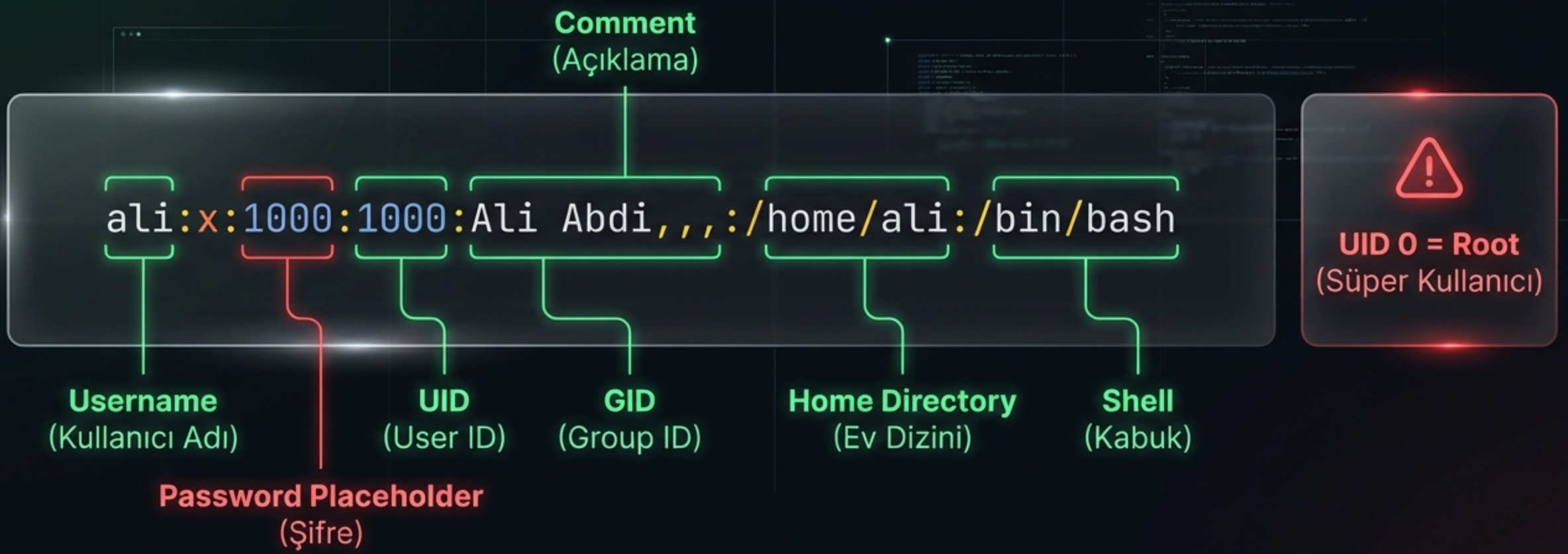
Savunmanın Temeli: **Kimlik ve Yetki**



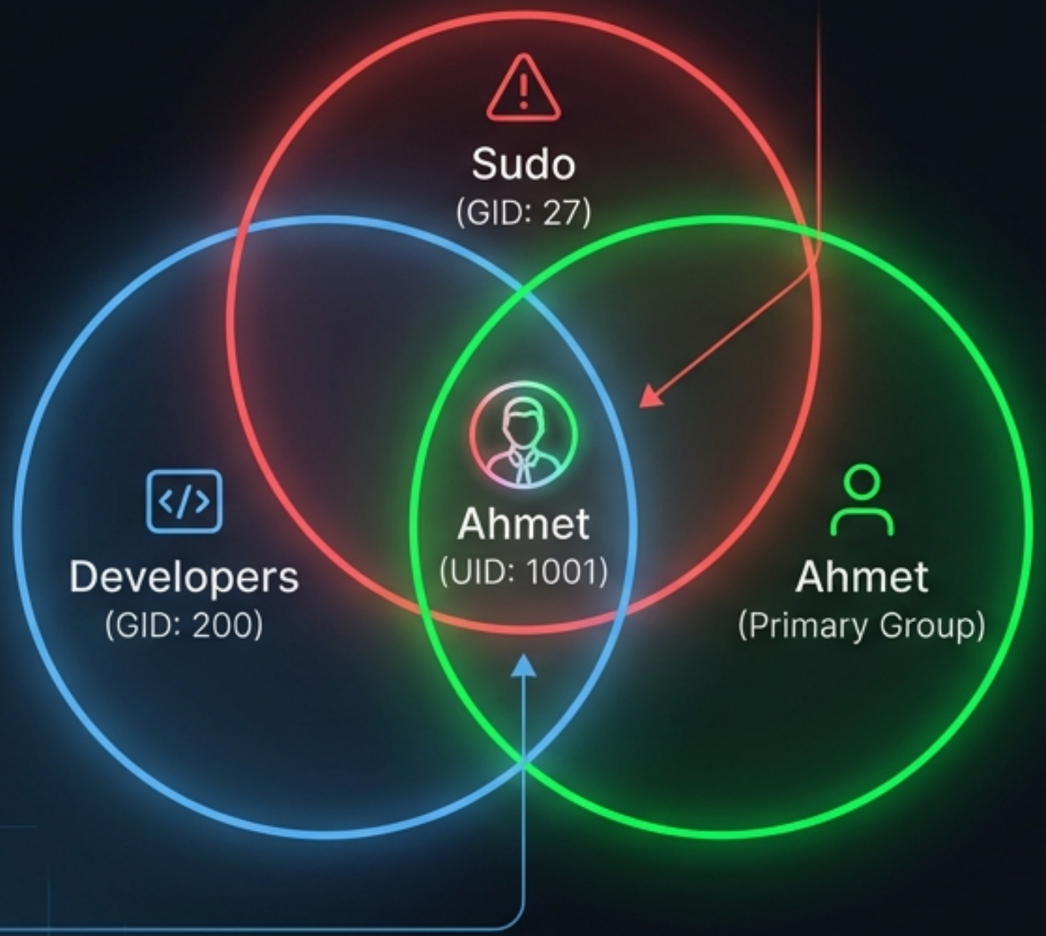
Kritik Uyarı: İzinler, sistemin ilk savunma hattıdır. Yanlış yapılandırma, siber "Privilege Escalation" (Yetki Yükseltme) riskini doğurur.

Linux Felsefesi: Çok kullanıcılı (Multi-user) mimari izolasyon gerektirir.

Kimlik Yönetimi: Kullanıcılar ve /etc/passwd



Organizasyon: Gruplar ve /etc/group

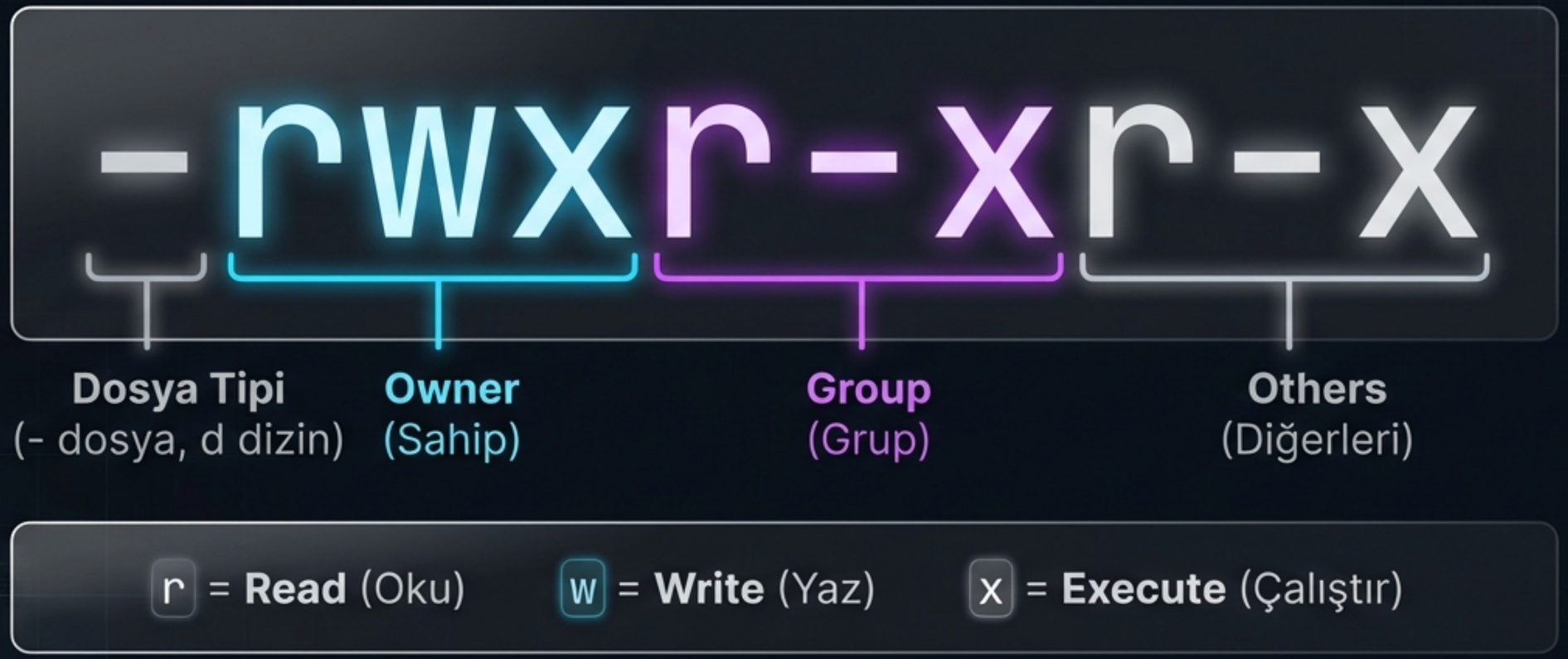



```
$ groups ahmet
ahmet : ahmet sudo developers

$ usermod -aG sudo ahmet
```

Veritabanı: /etc/group

İzinlerin Anatomisi: ls -l Okuryazarlığı



Temel İzin Türleri (r-w-x)

İzin Tipi (Değer)	Dosya	Dizin
 r (Read - 4)	İçeriği okuma (cat)	Dosyaları listeleme (`ls`)
 w (Write - 2)	Değiştirme/Silme	Dosya ekleme/silme
 x (Execute - 1)	Program çalıştırma	**İçine girme (cd)** `JetBrains Mono` ⚠ Dizinlerde 'x' olmadan içine girilemez!

Sahipliği Değiştirmek (chown)

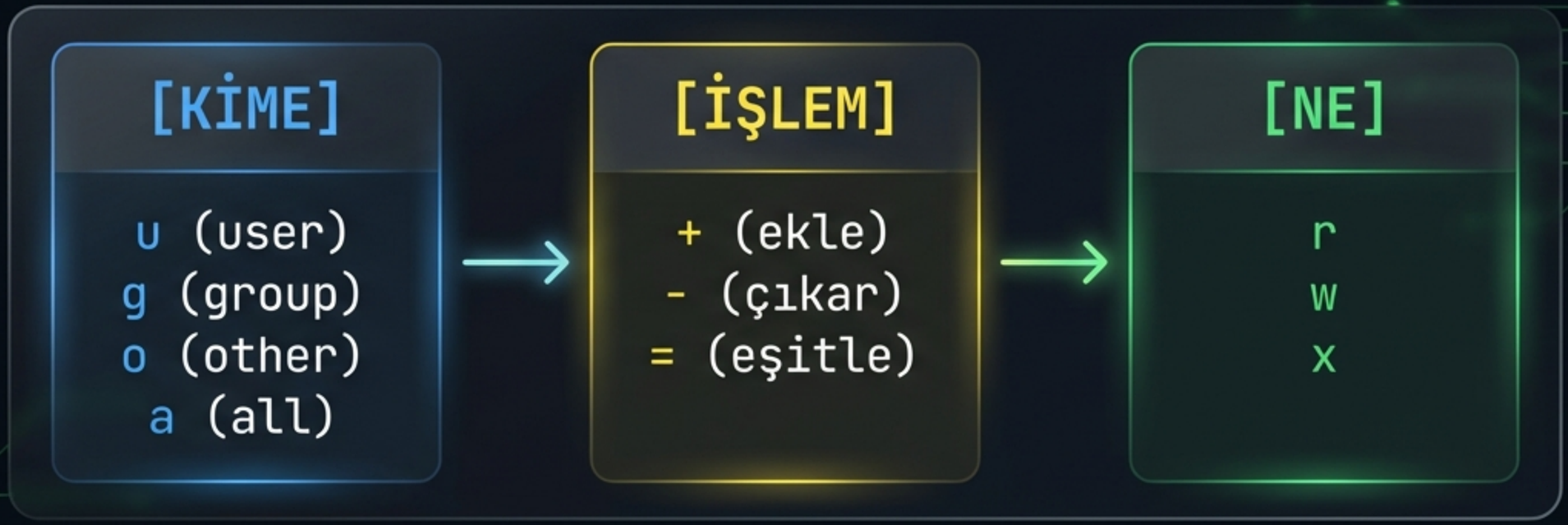

```
# chown ahmet:muhasebe rapor.txt
```

Yeni Sahip (User)

Yeni Grup (Group)

- `-R` : Klasör ve içindekileri (Recursive) değiştirir.

İzinleri Değiştirmek 1: Sembolik Mod




```
$ chmod g+w dosya.txt
(Gruba yazma izni ver)
```

```
$ chmod o-rwx gizli_dosya
(Diğerlerinin tüm haklarını al)
```

İzinleri Değiştirmek 2: Sayısal Mod (Octal)

Mathematics of Security

r (4) + w (2) + x (1) = 7

777
Danger/Everyone writes
`rwx rwx rwx`

755
Standard/Owner writes, others read
`rwx r-x r-x`

644
File/Owner reads/writes, others read
`rw- r-- r--`

Özel İzinler 1: SUID (Set User ID)

Temporary Authority

Normal Kullanıcı

Geçici Root Yetkisi

```
-rwsr-xr-x
```

SUID Bit (Special Permissions Location)

Siber Güvenlik Riski:

SUID bit unutulmuş dosyalar “Privilege Escalation” (Yetki Yükseltme) saldırılarına kapı açar.

Özel İzinler 2: SGID (Set Group ID)

drwxr-sr-x

SGID Bit (Grup Mirası)

Klasördeki her yeni dosya, otomatik olarak klasörün grubunu miras alır.

Özel İzinler 3: Sticky Bit


```
drwxrwxrwt
```

Sticky Bit (Kısıtlanmış Silme İzni)

```
chmod +t /tmp
```

Komut (Etkinleştirme)

Siber Güvenlik Perspektifi: Saldırı Vektörleri

Bilgi İfşası (Information Disclosure)

Hassas yapılandırma dosyalarında 'Others' okuma izni (o+r).

SUID İstismarı

Saldırganlar 'find / -perm -u=s' komutuyla root yetkisi veren dosyaları arar.

Kernel Exploit (Dirty COW)

Race Condition hatası ile salt-okunur dosyaların üzerine yazarak root olma (CVE-2016-5195).

En İyi Uygulamalar (Best Practices)

- Asla 'chmod 777' kullanmayın.
- Gereksiz SUID bitlerini temizleyin.

- Ev Dizinleri: chmod 700 (Sadece Sahibi)
- Web Dosyaları: chmod 644 (Sahip yazar, dünya okur)
- Web Dizinleri: chmod 755
- Config Dosyaları: chmod 600 (Sadece Root)

Prensip: Least Privilege (En Az Yetki)

Özet ve Referans Tablosu

Sayısal Değerler
7 (rwx) - Full permissions (read, write, execute)
5 (r-x) - Read and execute only
4 (r--) - Read only
0 (---) - No permissions

Özel İzinler
SUID (u+s) - Set User ID on execution
SGID (g+s) - Set Group ID on execution
Sticky (o+t) - Sticky bit (restricted deletion)

Temel Komutlar	
chmod	- Change file mode bits
chown	- Change file owner and group
chgrp	- Change group ownership
ls -l	- List directory content in long format

Güvenlik, doğru izinlerle başlar.