🔐 SİBER GÜVENLİK SÖZLÜĞÜ

A

AES (Advanced Encryption Standard)
Simetrik bir şifreleme algoritmasıdır. Günümüzde veri güvenliği için en yaygın kullanılan şifreleme standardıdır.

APT (Advanced Persistent Threat)
Devlet destekli veya yüksek organizasyonlu gruplar tarafından uzun süreli, hedef odaklı yapılan siber saldırılar.

Antivirüs
Zararlı yazılımları (malware) tespit eden, engelleyen ve temizleyen güvenlik yazılımı.

Authentication (Kimlik Doğrulama)
Bir kullanıcının gerçekten iddia ettiği kişi olduğunu doğrulama süreci.

Authorization (Yetkilendirme)
Kimliği doğrulanmış kullanıcının hangi kaynaklara erişebileceğinin belirlenmesi.

B

Backdoor (Arka Kapı)
Sisteme gizli ve yetkisiz erişim sağlayan güvenlik açığı veya kötü amaçlı mekanizma.

Backup (Yedekleme)
Verilerin kaybolma riskine karşı kopyalanması.

Botnet
Zararlı yazılım bulaşmış cihazlardan oluşan ve uzaktan kontrol edilen ağ.

Brute Force Attack
Şifreyi deneme-yanılma yöntemiyle kırmaya yönelik saldırı.

C

C&C (Command and Control)
Saldırganın ele geçirilmiş sistemleri yönettiği kontrol sunucusu.

CIA Triadı (Confidentiality, Integrity, Availability)
Bilgi güvenliğinin üç temel prensibi:

- Gizlilik

- Bütünlük
- Erişilebilirlik

Cryptography (Kriptografi)
Bilgiyi yetkisiz erişime karşı koruma bilimi.

CSRF (Cross-Site Request Forgery)
Kullanıcının bilgisi olmadan yetkili olduğu bir işlem yaptırılmasını sağlayan web saldırısı.

D

DDoS (Distributed Denial of Service)
Bir sistemi aşırı trafikle hizmet veremez hale getirme saldırısı.

Digital Signature (Dijital İmza)
Verinin kaynağını ve bütünlüğünü doğrulayan kriptografik imza.

DNS Spoofing
Kullanıcıyı sahte bir web sitesine yönlendirme saldırısı.

Data Breach (Veri İhlali)
Yetkisiz kişilerin hassas verilere erişmesi.

E

Encryption (Şifreleme)
Veriyi okunamaz hale getirerek koruma işlemi.

Endpoint Security
Bilgisayar, telefon gibi uç cihazların korunması.

Exploit
Bir güvenlik açığını kullanarak sisteme sızma yöntemi.

F

Firewall (Güvenlik Duvarı)
Ağ trafiğini filtreleyerek yetkisiz erişimi engelleyen sistem.

Forensics (Adli Bilişim)
Siber olay sonrası dijital delillerin incelenmesi.

Phishing (Oltalama)
Kullanıcıyı kandırarak hassas bilgilerini ele geçirme yöntemi.

H

Hash Function (Özet Fonksiyonu)
Veriyi sabit uzunlukta bir değere dönüştüren kriptografik fonksiyon.

Honeypot
Saldırganları tuzağa düşürmek için oluşturulmuş sahte sistem.

HTTP vs HTTPS
HTTPS, SSL/TLS ile şifrelenmiş güvenli web iletişimidir.

I

IDS (Intrusion Detection System)
Saldırıları tespit eden sistem.

IPS (Intrusion Prevention System)
Saldırıları tespit edip engelleyen sistem.

IAM (Identity and Access Management)
Kimlik ve erişim yönetimi süreçleri.

K

Keylogger
Klavye tuşlarını kaydeden zararlı yazılım.

KPI (Key Performance Indicator)
Güvenlik performansını ölçmek için kullanılan metrik.

M

Malware
Zararlı yazılımların genel adı (virüs, trojan, ransomware vb.).

Man-in-the-Middle (MITM)
İki taraf arasındaki iletişimi gizlice dinleme veya değiştirme saldırısı.

MFA (Multi-Factor Authentication)
Çok faktörlü kimlik doğrulama (şifre + SMS kodu gibi).

P

Patch (Yama)
Yazılımdaki güvenlik açığını kapatmak için yayımlanan güncelleme.

Penetration Test (Sızma Testi)
Sistemin güvenliğini test etmek için yapılan kontrollü saldırı.

Privilege Escalation
Yetki yükseltme saldırısı.

R

Ransomware
Verileri şifreleyip fidye isteyen zararlı yazılım.

Risk Assessment (Risk Analizi)
Tehdit ve zafiyetlerin değerlendirilmesi süreci.

Rootkit
Sistemde gizlenerek kalıcı erişim sağlayan zararlı yazılım.

S

SIEM (Security Information and Event Management)
Güvenlik olaylarını toplayan ve analiz eden sistem.

SOC (Security Operations Center)
Güvenlik operasyonlarının yürütüldüğü merkez.

SQL Injection
Veritabanına zararlı SQL komutları gönderme saldırısı.

Social Engineering (Sosyal Mühendislik)
İnsanları manipüle ederek bilgi elde etme yöntemi.

SSL/TLS
Güvenli veri iletimi sağlayan kriptografik protokoller.

T

Trojan (Truva Atı)
Kendini zararsız gösteren zararlı yazılım.

Threat Intelligence (Tehdit İstihbaratı)
Güncel tehditler hakkında toplanan bilgi.

V

VPN (Virtual Private Network)
İnternet trafiğini şifreleyerek güvenli bağlantı sağlayan sistem.

Vulnerability (Zafiyet)
Sistemde bulunan güvenlik açığı.

X

XSS (Cross-Site Scripting)
Web uygulamasına zararlı script enjekte etme saldırısı.

📌 İleri Seviye Terimler

Zero-Day
Henüz üretici tarafından bilinmeyen ve yaması olmayan güvenlik açığı.

Zero Trust
Hiçbir kullanıcı veya cihazın varsayılan olarak güvenilir kabul edilmediği güvenlik modeli.

Sandboxing
Şüpheli yazılımı izole bir ortamda çalıştırma yöntemi.

Red Team / Blue Team

- Red Team: Saldırı simülasyonu yapan ekip
- Blue Team: Savunma yapan ekip