**MITRE ATT&CK NAVIGATOR**

**1. Nedir?**  
MITRE ATT&CK Navigator, siber saldırıların **taktiklerini ve tekniklerini görsel olarak haritalamak** için kullanılan bir araçtır.  
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), dünyadaki saldırganların nasıl davrandığını gösteren büyük bir veritabanıdır.  
**Navigator**, bu veritabanı üzerinde çalışır ve bu teknikleri görsel olarak incelemeni sağlar.

Kısaca:  
- "Saldırganlar hangi yolları kullanıyor?"  
- "Bu yolları tablo olarak göster."  
- "Kendine göre işaretle, analiz et."



**2. Ne İşe Yarar?**

* Siber saldırıların nasıl gerçekleştiğini anlamak için kullanılır.
* Güvenlik ekipleri, saldırganların kullandığı yöntemleri bu tabloya göre takip eder.
* Belirli bir saldırıya karşı sistemin ne kadar savunmasız olduğunu görebilirsin.
* Red Team, Blue Team ve tehdit avcıları (threat hunters) için çok değerlidir.

➡️ Saldırının hangi aşamada hangi teknik kullanıldığını görebilir, kendi analiz tablonu oluşturabilirsin.

**3. Neden Önemlidir?**

* Saldırılar her zaman karmaşıktır, ama MITRE ATT&CK bu karmaşıklığı düzenler.
* Güvenlik uzmanları sistemlerini hangi tekniklere karşı koruması gerektiğini bu tabloya bakarak anlar.
* Şirketler, “hangi saldırı tekniğine karşı önlemim eksik?” sorusuna Navigator sayesinde kolayca cevap bulur.
* Eğitim, savunma planlaması ve saldırı simülasyonlarında çok kullanılır.

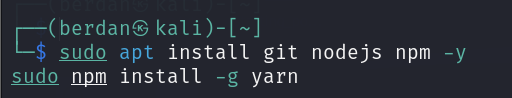
**4. Nasıl Kurulur? (Linux Örneği)**

MITRE ATT&CK Navigator web tabanlıdır ama istersen kendi bilgisayarına da kurabilirsin.

**# 1. Gerekli yazılımlar: git, nodejs, yarn**

**sudo apt install git nodejs npm -y**

**sudo npm install -g yarn**



**# 2. Navigator’ü indir**

**git clone https://github.com/mitre-attack/attack-navigator.git**

**cd attack-navigator/nav-app**

****

**# 3. Kur ve başlat**

**yarn install**

**yarn start**

Artık tarayıcıdan **http://localhost:4200** adresine giderek kendi Navigator ekranını görebilirsin.

Alternatif olarak hiç kurmadan şu adresten online da kullanabilirsin:  
🔗 https://mitre-attack.github.io/attack-navigator/

**5. Örnek Bir Anlatım:**  
Diyelim ki bir saldırgan şirketteki bir bilgisayara kötü amaçlı yazılım yükledi. Sonra şu adımları yaptı:

1. Erişim kazandı (Initial Access)
2. Kimlik bilgilerini çaldı (Credential Access)
3. Uzaktan kontrol sağladı (Command and Control)

Sen bu saldırıyı analiz ederken MITRE ATT&CK Navigator’ü açarsın, ilgili teknikleri **tablo üzerinde renklendirerek** işaretlersin.

Bu sayede şunları görebilirsin:

* Saldırı hangi aşamalardan oluştu?
* Hangi teknikler kullanıldı?
* Bunlara karşı sistemde savunma var mı?

Böylece eksik savunmaları belirler, önlem alırsın.

**Uyarı:**  
MITRE ATT&CK Navigator bir saldırı aracı değil, bir analiz ve görselleştirme aracıdır. Güvenlik testleri ve savunma stratejileri için kullanılır. Yanlış anlamalara yol açmaması için dikkatli anlatılmalıdır.