## **Atomic Red Team Nedir, Neden Kullanılır?**

**Atomic Red Team**, MITRE ATT&CK Framework’e dayalı olarak hazırlanmış, **basit, izole ve tekrarlanabilir saldırı simülasyonları** içeren bir açık kaynak test koleksiyonudur. Red Team, Blue Team ve Purple Team ekipleri tarafından; savunma sistemlerinin zafiyetlere ve davranışsal tehditlere karşı ne derece etkili olduğunu test etmek amacıyla kullanılır.

Atomic Red Team’in temel amacı, güvenlik analistlerinin veya mavi takım (Blue Team) üyelerinin, bir saldırı simülasyonunu kolayca çalıştırıp bunun **EDR, SIEM ya da log toplama sistemleri tarafından yakalanıp yakalanmadığını** test etmesini sağlamaktır. Bu sayede kullanılan güvenlik araçlarının görünürlük düzeyi ve alarm üretme kabiliyeti değerlendirilir.

Her "atomic test", MITRE ATT&CK matrisindeki bir teknikle eşleştirilmiştir (örneğin: T1059 – Command and Scripting Interpreter, T1003 – Credential Dumping). Her test küçük, bağımsız ve sistem üzerinde tehlike yaratmayacak şekilde tasarlanmıştır. Bu da güvenli ortamda test yapılmasına olanak tanır.

## Kurulum

Atomic Red Team kendisi bir araç değil, **test senaryoları koleksiyonudur**. Bu testleri kolayca çalıştırmak için en çok tercih edilen yöntem, [Invoke-AtomicRedTeam](https://github.com/redcanaryco/invoke-atomicredteam) PowerShell scriptidir.

Kurulum adımları (Windows PowerShell için):

* git clone https://github.com/redcanaryco/atomic-red-team.git
* cd atomic-red-team
* Set-ExecutionPolicy Bypass -Scope Process
* Import-Module .\atomics\Invoke-AtomicRedTeam.psd1

## **Kullanım Örneği**

PowerShell üzerinden örnek bir test çalıştırmak için:



Bu komut, **MITRE ATT&CK T1059.001** (PowerShell ile komut yürütme) tekniğine karşılık gelen atomic testleri listeler. Çalıştırmak için:



* -TestNumbers → Hangi testi çalıştıracağını belirtir.
* -ConfirmFalse → Test öncesi kullanıcı onayı istemez (otomatik çalıştırma).

## **Elde Edilebilecek Bilgiler ve Etkiler**

Atomic Red Team testleriyle aşağıdaki alanlarda görünürlük ve savunma testi yapılabilir:

* Komut satırı saldırı davranışları
* Credential dumping (şifre, hash) denemeleri
* PowerShell, WMI, Windows Services suistimalleri
* Persistence teknikleri (örneğin RunKey, Scheduled Tasks)
* Network discovery, lateral movement senaryoları
* UAC bypass, DLL injection gibi teknik davranışlar

Bu testler doğrudan saldırı gerçekleştirmez; sadece davranışları taklit ederek savunma sistemlerinin tepkisini ölçer.

## Parametreler ve Özellikler

**Invoke-AtomicRedTeam** modülü ile en sık kullanılan komutlar şunlardır:

* Invoke-AtomicTest <TechniqueID> → Test çalıştır
* Get-AtomicTechnique → Tüm teknikleri listeler
* Search-AtomicTests keyword → Belirli terimle eşleşen testleri arar
* Get-AtomicPrereqs → Test için ön koşulları gösterir
* Invoke-AtomicTest -Cleanup → Test sonrası ortamı temizler
* -InputArgs → Teste özel parametre aktarımı

Atomic Red Team, saldırı simülasyonu yapmak isteyen Red, Blue veya Purple Team'ler için hızlı, pratik ve kontrollü bir çözümdür. Gerçek zararlı yazılım kullanmadan, yalnızca davranış benzerliği üzerinden sistemlerin ne kadar izleme ve uyarı verebildiği test edilebilir. Özellikle MITRE ATT&CK Framework’ü temel alan savunma mimarileri için vazgeçilmez bir test aracıdır.