**Atomic Red Team**, MITRE ATT&CK framework’ü kapsamında tanımlanan saldırı tekniklerinin **basitleştirilmiş, kontrollü ve test edilebilir örneklerini (atomik testler)** sunan açık kaynaklı bir siber güvenlik test çerçevesidir.

Savunma sistemlerini test etmek, algılama kurallarını doğrulamak, SOC ekiplerinin reflekslerini ölçmek gibi amaçlarla kullanılır.

**Bu Aracın Özellikleri Nelerdir?**

* **MITRE ATT&CK uyumlu**: Tactics/Techniques/Procedures (TTPs) ile eşleşir.
* **Atomik Testler**: Her teknik için minimal ve anlaşılır test dosyaları içerir.
* **Platform Desteği**: Windows, Linux, macOS.
* **PowerShell ile Entegrasyon**: Invoke-AtomicRedTeam modülü ile çalıştırılabilir.
* **Detection Engineering ve SOC eğitimi için ideal**
* **Yalın YAML formatında tanımlamalar**
* **Sigma, Splunk ve Elastic ile entegrasyon desteği**

**Atomic Red Team Aracını Kali Linux veya Windows Üzerinde Kullanma Adımları**

**Adım 1: PowerShell ile Atomic Red Team’i Klonlayın**

“git clone https://github.com/redcanaryco/atomic-red-team.git”

”cd atomic-red-team”

**Adım 2: PowerShell Modülünü Yükleyin (Invoke-AtomicRedTeam)**

“Install-Module -Name Invoke-AtomicRedTeam -Force

Import-Module Invoke-AtomicRedTeam”

**Adım 3: Ortamı Hazırla (İlk Kurulum Scripti)**

“Invoke-AtomicRedTeam -Setup”

**Adım 4: Teknik Listelemesi (Tüm Atomic Testleri Gör)**

“Get-AtomicTechnique”

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 5: Belirli Bir Saldırı Tekniğini Çalıştırma**

Örnek: **T1059.001 – PowerShell Komutları Çalıştırma**

“Invoke-AtomicTest T1059.001 -ShowDetails”

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

Testi çalıştırmak için komut:

“Invoke-AtomicTest T1059.001 -TestNumbers 1 -ConfirmFalse”

**Adım 6: Linux veya Bash Tabanlı Test (Kali)**

Örnek teknik: **T1082 – Sistem Bilgisi Toplama**

“cat atomics/T1082/T1082.yaml”

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

Manual çalıştırmak için komut :

“uname -a && hostname”