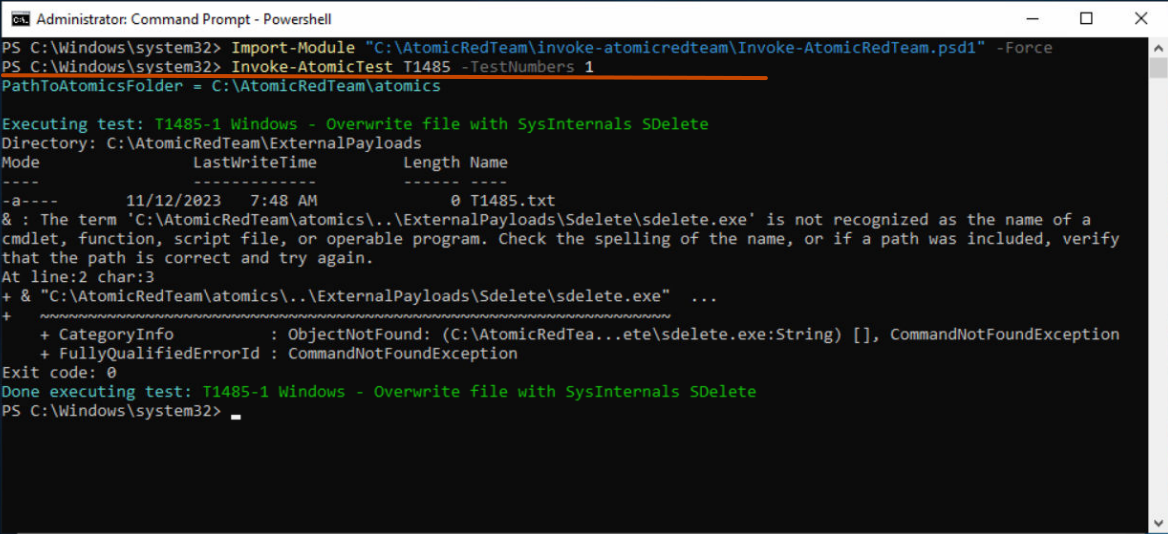
**Atomic Red Team Nedir?**

**Atomic Red Team**, gerçek hayattaki siber saldırıların küçük ve kontrol edilebilir (yani zararsız) kopyalarını çalıştırmamıza olanak sağlayan bir test ve eğitim aracıdır.

Atomic Red Team, “gerçek saldırılar gibi ama zararsız” küçük testler çalıştırarak sistemin verdiği tepkileri gözlemlememizi sağlar.



Atomic testlerin detaylarının görüntülendiği ve ön koşulların kontrol edilmesine dair bölümler.

**Ne İşe Yarar?**

Atomic Red Team ile:

* Bir saldırgan gibi belirli teknikleri test edebilirsin
* Bir güvenlik sistemi (örneğin antivirüs veya EDR) bu testleri yakalıyor mu görebilirsin
* SOC ekiplerinin veya SIEM sistemlerinin alarm üretip üretmediğini test edebilirsin
* Öğrenciler, gerçek saldırı örneklerini risk olmadan gözlemleyebilir

**Atomic Red Team Nasıl Kurulur?**

Atomic Red Team aslında bir koleksiyondur. Testler, PowerShell komutları veya betikler şeklindedir.

Kullanmak için önerilen yol Invoke-AtomicRedTeam adlı PowerShell betiğini kullanmaktır.

**Gerekli Ön Koşullar**

* PowerShell 5 veya üstü
* Windows 10 veya üstü (tercihen sanal makine!)
* Admin yetkileri (bazı testler için)

**Kurulum Adımları (Windows)**

PowerShell’i Yönetici Olarak Aç:

Script çalıştırmaya izin ver:

***Set-ExecutionPolicy Bypass -Scope Process***

***Set-ExecutionPolicy Bypass -Scope Process***

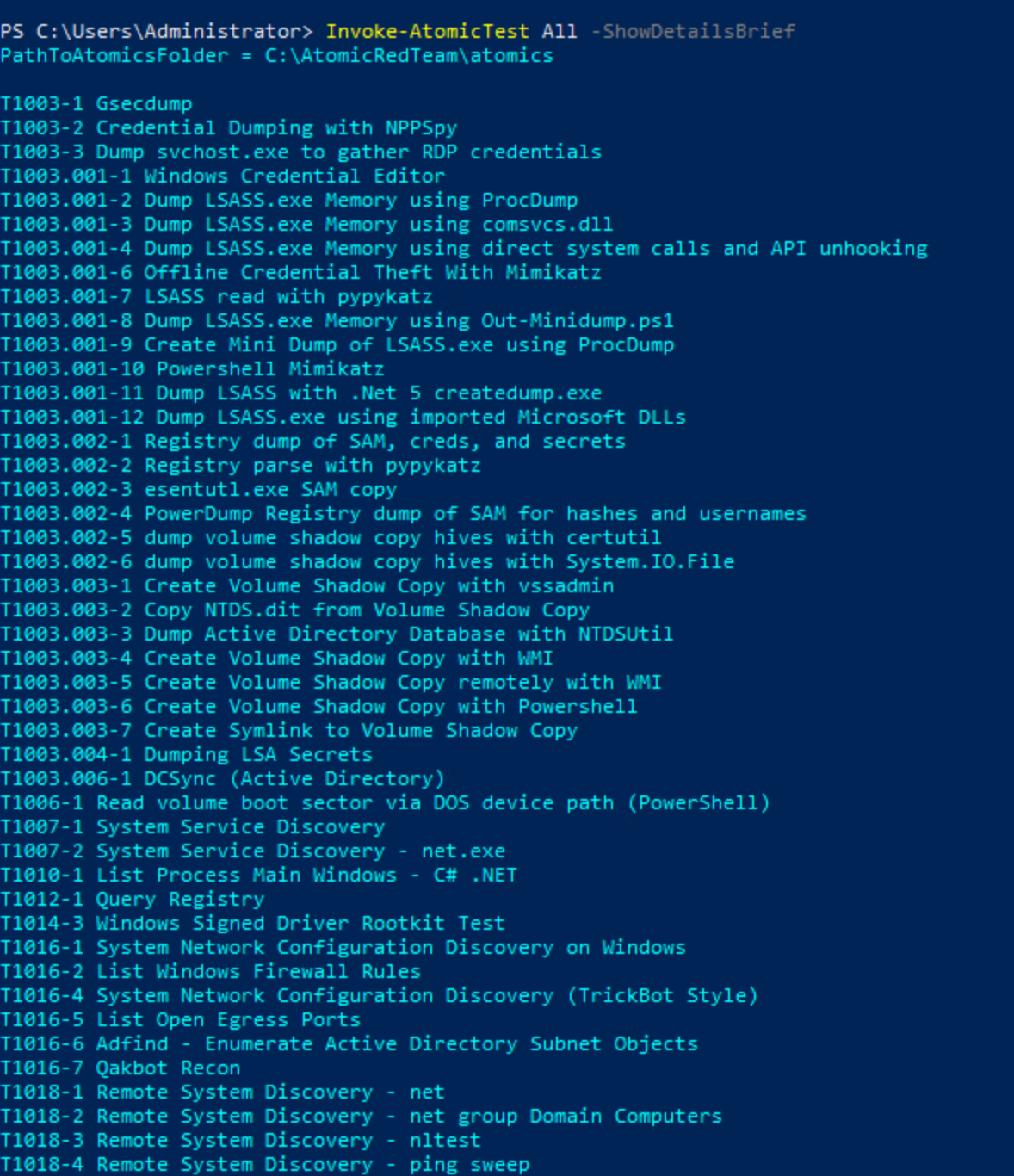
Invoke-AtomicRedTeam betiğini indir:

***Install-Module -Name Invoke-AtomicRedTeam -Force***

Betiği içe aktar: ***Import-Module Invoke-AtomicRedTeam***

Atomic Test veritabanını indir

***Invoke-AtomicRedTeam -GetAtomics***

******

**Avantajlar ve Sınırlamalar**

**Avantajları:**

* Açık kaynak ve ücretsiz
* Gerçek saldırı davranışlarını simüle eder
* SIEM ve EDR testleri için mükemmeldir
* MITRE ATT&CK ile uyumludur

**Dikkat Edilmesi Gerekenler:**

* Bazı testler riskli olabilir → her zaman sanal makinede çalıştırılmalıdır!
* Yönetici hakları gerekebilir
* Türkçe arayüz yok

Atomic Red Team, siber güvenlik öğrenenler için saldırı tekniklerini güvenli ve kontrollü biçimde test etme imkânı sunar. Lise düzeyinde siber güvenlik eğitimi alan öğrenciler, bu araçla hem MITRE ATT&CK kavramını öğrenir hem de pratik yaparak olayların nasıl algılandığını gözlemleyebilir.

Gerçek saldırılar gibi çalışan ama kimseye zarar vermeyen bu testler, eğitim için idealdir.