BadBlood - Active Directory (AD) Eğitim Materyali

# 🔍 BadBlood Nedir?

BadBlood, Active Directory (AD) ortamlarını eğitim ve test amaçlı sahte (dummy) kullanıcılar, gruplar, izinler ve politikalarla doldurmak için kullanılan açık kaynaklı bir araçtır.   
Özellikle siber güvenlik eğitimlerinde ve saldırı simülasyonlarında gerçekçi bir AD ortamı yaratmak için kullanılır.

# 🔧 Özellikleri

- Eğitim ve saldırı simülasyonları için sahte AD ortamı oluşturur.  
- Kullanıcılar, gruplar, OU'lar, GPO'lar vb. objeler ekler.  
- Gerçekçi ilişkiler kurar: kullanıcı-grup, grup-GPO vs.  
- Powershell ile çalışır, komut satırından yönetilir.  
- Hem küçük hem büyük AD ortamları kurmak mümkündür.

# 📌 Kullanım Alanları

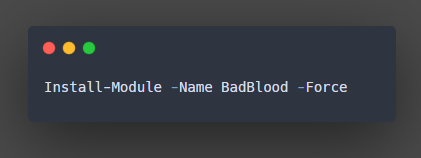
- Red Team eğitimleri  
- Blue Team tespit senaryoları  
- Adli analiz ve olay müdahale eğitimleri  
- Active Directory saldırı tekniklerinin test edilmesi

# 💻 Kurulum Adımları

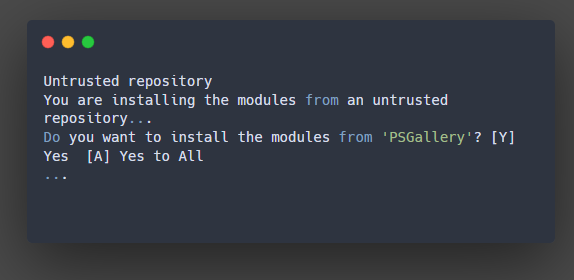
BadBlood, Windows ortamında PowerShell üzerinden çalıştırılır. İşte adım adım kurulum:

1. PowerShell'i yönetici olarak çalıştırın.

2. Gerekli modülleri yükleyin:

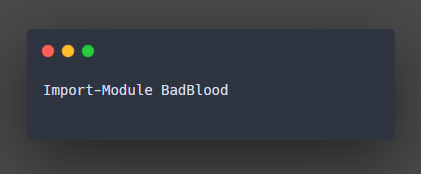


**Açıklama:** PowerShell için BadBlood modülünü indirir ve yükler.

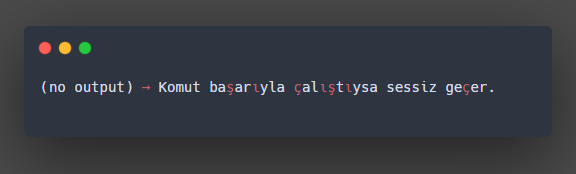


✅ Devam etmek için Y veya A tuşuna basılır.

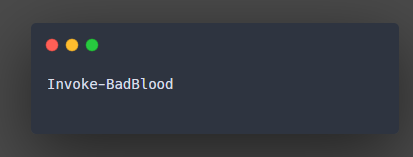
3. Modülü içe aktarın:



**Açıklama:** Yüklenen modülü aktif hale getirir. Her oturumda bir kez çalıştırılır.



4. AD içeriğini oluşturmak için çalıştırın:



# 

✅ Bu işlem birkaç dakika sürebilir. Ardından AD ortamınız test için hazır hale gelir.

# 🚀 Kullanım Senaryosu

Bir Windows Server ortamında Domain Controller kuruluysa, BadBlood ile bu ortama kullanıcılar ve gruplar oluşturabilirsiniz.  
Ardından bu AD verisi ile BloodHound gibi araçlar üzerinde analiz yapabilir ya da Red Team testleri gerçekleştirebilirsiniz.