BlueToolkit Nedir ve Nasıl Kullanılır?

# 📌 BlueToolkit Nedir?

BlueToolkit, genellikle Active Directory (AD) güvenliğiyle ilgili kullanılan bir savunma (Blue Team) araç takımıdır. Ancak 'PingCastle' gibi yaygın, bağımsız ve standart bir araç olarak genel kabul görmüş bir araç değildir. BlueToolkit ismi, bazı kurum içi projeler, eğitim içerikleri veya özel script setleri için kullanılan genel bir isim olabilir.

# 🎯 Olası Anlamlar:

## 1. Red Team / Blue Team Eğitimlerinde Kullanılan Araç Seti

BlueToolkit bazı eğitim veya güvenlik ekipleri tarafından, Blue Team savunma araçlarını bir araya getiren bir seti ifade eder. İçeriğinde şu araçlar bulunabilir:

- PingCastle: AD sağlık kontrol aracı  
- BloodHound: Active Directory ilişkileri analiz aracı  
- Sysmon + ELK: Log toplama ve analiz platformu  
- Winlogbeat, Zeek, Suricata: Ağ ve olay izleme araçları  
- LAPS GUI: Local Admin Password Solution yönetim aracı  
- Group Policy Analyzer: GPO yapı analiz aracı

## 2. GitHub Tabanlı veya Kuruma Özel Geliştirme Projeleri

GitHub üzerinde veya kurum içi özel geliştirilen bazı projelerde 'BlueToolkit' adı kullanılabilir. Bu araçlar genellikle PowerShell scriptlerinden, log analiz scriptlerine kadar geniş bir içerik barındırır.

# 📘 BlueToolkit Kullanımı (Varsayımsal)

Komut Örneği:

BlueToolkit.exe --mode audit --target-domain corp.local

ekran görüntüsü, yazı tipi, metin, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Terminal Çıktısı Örneği:

# *metin, ekran görüntüsü, yazı tipi içeren bir resim Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.*📎 Sonuç

BlueToolkit adı, şu anda yaygın bir açık kaynak güvenlik aracı olarak öne çıkmasa da, birçok kurumun iç araç setinde veya eğitim materyalinde Blue Team için geliştirilen araç topluluğu olarak kullanılmaktadır. Eğer özel bir kaynak, dosya veya ekran görüntüsüne sahipseniz, neye atıfta bulunduğunuzu netleştirebilirim.