**CrackMapExec (CME) Nedir?**

CrackMapExec, Python tabanlı, çok fonksiyonlu bir Active Directory (AD) saldırı aracıdır.  
Ağ üzerinde kimlik bilgileri denemek, SMB, RDP ve WinRM gibi servislerde zafiyet taramak, kullanıcı/şifre kombinasyonlarını test etmek ve etki alanı içerisinde ilerlemek için kullanılır.  
Red Team'lerin ve iç ağ sızma testi uzmanlarının vazgeçilmez araçlarından biridir.

CME, temel olarak “Living off the Land” (LoTL) felsefesine dayanır; yani hedef ağda mevcut protokolleri ve yapı taşlarını kullanarak hareket eder.

**CrackMapExec Ne İşe Yarar?**

* SMB, RDP, WinRM, MSSQL gibi protokoller üzerinden hedef sistemlere erişim dener.
* Kimlik bilgisi (kullanıcı/şifre veya hash) test eder.
* Active Directory kullanıcılarını, paylaşımları, grup bilgilerini çeker.
* Zafiyetli servisleri ve yanlış yapılandırmaları tespit eder.
* Post-exploitation işlemler (örneğin: komut çalıştırma, payload gönderme) yapılabilir.
* Spray saldırıları ve hash üzerinden kimlik doğrulama testleri yapılabilir.

**Kurulum (Kali Linux için)**

***sudo apt install crackmapexec***

Veya GitHub üzerinden:

***git clone https://github.com/Porchetta-Industries/CrackMapExec***

***cd CrackMapExec***

***pip3 install -r requirements.txt***

***python3 setup.py install***

**Temel Kullanım Komutları**

1. Ağ taraması yapma:

***crackmapexec smb 192.168.1.0/24***

1. Kullanıcı ve parola ile kimlik doğrulama testi:

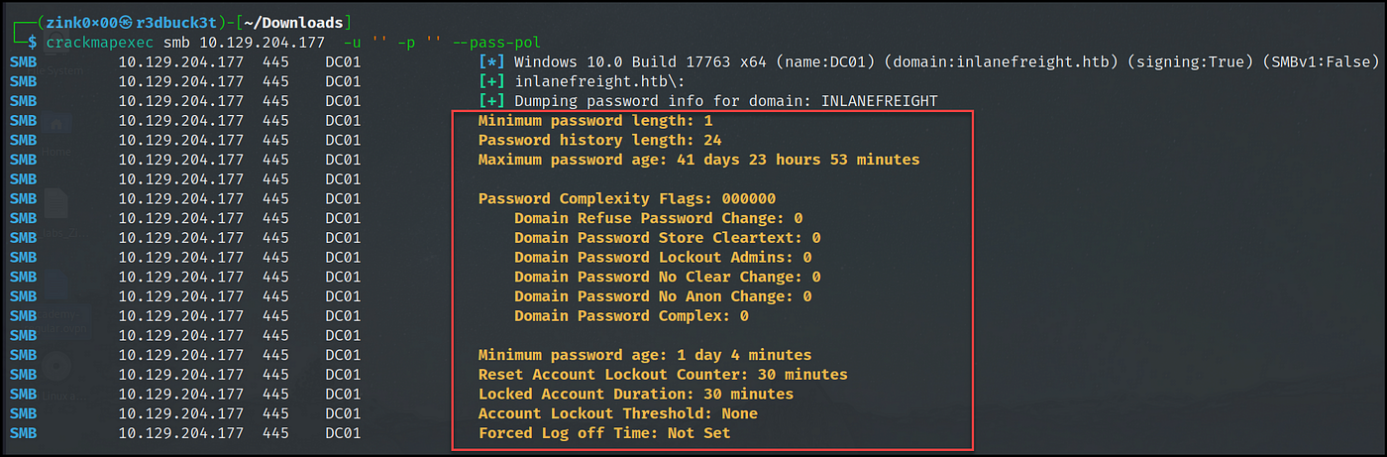
***crackmapexec smb 192.168.1.100 -u admin -p Password123***

1. Hash üzerinden bağlantı testi (Pass-the-Hash):

***crackmapexec smb 192.168.1.100 -u administrator -H aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c***

1. Komut çalıştırma (komut çıktısını alır):

***crackmapexec smb 192.168.1.100 -u admin -p Password123 -x 'whoami'***

******

Tipik bir kullanımda şöyle bir komut çalıştırılır:

***crackmapexec smb 192.168.1.0/24***

**Eğitim Notları**

CrackMapExec, öğrencilere Active Directory ortamlarında nasıl bilgi toplandığını, saldırıların nasıl otomatikleştirildiğini ve ağ içi yayılmanın nasıl gerçekleştiğini öğretmek için harika bir araçtır. Hem saldırı yüzeyini genişletir hem de kimlik bilgisi testleriyle yanlış yapılandırmaları ortaya çıkarır.

CrackMapExec, sadece bilgi toplamakla kalmaz; aynı zamanda ele geçirilen kimlik bilgileri ile sistemler üzerinde komut çalıştırma ve etki alanında **lateral movement** (yatay geçiş) yapma gibi adımları da mümkün kılar. Bu yönüyle CME, bir sistemde elde edilen yetkinin tüm ağa yayılmasını test etmek için kullanılır.

Ayrıca, arka planda **Impacket** kütüphanesini kullanarak birçok Windows protokolünü doğrudan yönetir. Bu da onu hem güçlü hem de hafif bir çözüm haline getirir. Red Team senaryoları, CTF yarışmaları veya laboratuvar ortamları için CrackMapExec vazgeçilmezdir.