**🔍 1. CrackMapExec Nedir?**

**CrackMapExec (CME)**, özellikle **Active Directory ortamlarında** kullanılan, güçlü bir **post-exploitation** ve **penetrasyon testi** aracıdır.

* SMB (Windows dosya paylaşımı) protokolü üzerinde çalışır
* Zayıf şifreleri test eder (brute-force değil, parola deneme)
* Kullanıcı adı/parola kombinasyonlarını dener
* Yetenekleri sayesinde ağ keşfi, kullanıcı oturumları, yetki tespiti ve RCE gibi işlemleri gerçekleştirebilir

🧰 **2. Kurulum (Kali Linux)**

Kali Linux’ta yüklü gelmeyebilir. Kurmak için:

bash

KopyalaDüzenle

sudo apt update

sudo apt install crackmapexec

metin, yazı tipi, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

🖥️ **3. Temel Komutlar ve Kullanım**

✅ **1. Ağda SMB ile tarama (versiyon bilgisi almak):**

cme smb 192.168.1.0/24

Ağdaki makinelerin SMB servis durumunu listeler.

✅ **2. Kullanıcı adı/parola ile giriş test etmek:**

cme smb 192.168.1.100 -u administrator -p 123456

Giriş başarılıysa “Pwned!” mesajı alınır. Aksi takdirde reddedilir.

✅ **3. Parola listesini denemek:**

cme smb 192.168.1.100 -u administrator -p passwords.txt

passwords.txt içinde denenmesini istediğin parolalar sıralanır.

✅ **4. Kullanıcı listesi ile birlikte parola test etmek:**

bash

KopyalaDüzenle

cme smb 192.168.1.100 -u users.txt -p passwords.txt

* users.txt → kullanıcı adları
* passwords.txt → şifreler

✅ **5. Oturum açmış kullanıcıları görüntülemek:**

bash

KopyalaDüzenle

cme smb 192.168.1.100 -u admin -p 123456 --sessions

Hedef sistemde aktif oturum açmış kullanıcıları gösterir.

✅ **6. Komut çalıştırmak (RCE):**

bash

KopyalaDüzenle

cme smb 192.168.1.100 -u admin -p 123456 -x "ipconfig"

Eğer kullanıcı gerekli yetkiye sahipse komut çalıştırılır, çıktı alınır.

metin, ekran görüntüsü, multimedya yazılımı, yazılım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧪 4. Uygulama Senaryosu (Sınıf Ortamı)**

1. Öğrenciler sanal Windows makinelerini yerel ağa bağlar.
2. Kali Linux kullanan öğrenci cme smb ile tüm makineleri tarar.
3. Belirlenen kullanıcı adı ve şifre kombinasyonları test edilir.
4. Başarılı giriş sonrası komut çalıştırılır (örnek: whoami, ipconfig)
5. Etik kurallar dahilinde gerçek sistemlere zarar verilmeden uygulama yapılır.

**🎯 . Öğrenim Çıktıları**

* Active Directory ortamlarında kimlik doğrulama testleri
* SMB protokolü nasıl çalışır
* Hangi kullanıcılar hangi erişimlere sahip
* Yetkisiz erişimin sistemde yaratabileceği sonuçlar
* Etik hackerlıkta sömürü araçlarının doğru kullanımı

**📌 . Ekstra Notlar**

* CME sadece SMB değil; **RDP**, **WINRM**, **MSSQL**, **LDAP** gibi diğer protokolleri de destekler.
* Modüller ile entegre çalışabilir (örneğin **Mimikatz**, **kerberos**, vs.)
* Dosya yükleme, servis başlatma, token bilgisi alma gibi ileri düzey fonksiyonlar sunar