**Responder**

**1. Nedir?**

**Responder**, yerel ağda (örneğin okul, şirket, internet kafesi gibi aynı Wi-Fi ağı) bulunan bilgisayarların kimlik bilgilerini (şifre karması - hash) yakalamaya yarayan bir **ağ dinleme (sniffing)** ve **kimlik avı** aracıdır.  
Kısaca: “Ağdaki şifreleri dinler ve toplar.”



**2. Ne işe yarar?**

* Responder, ağdaki bilgisayarlar bir **sunucu ararken** (örneğin bir dosya paylaşımı yaparken), onları kandırır ve kendini o sunucu gibi gösterir.
* Böylece, kullanıcılar fark etmeden **şifrelerini (hash) Responder’a gönderir.**
* Bu hash'ler sonra **kırılabilir** (örneğin John the Ripper ile).

**3. Neden önemlidir?**

* Kurumsal ağlarda en çok yapılan saldırılardan biri **LLMNR/NBT-NS spoofing**dir.
* Responder bu zayıflığı kullanarak ağdaki kullanıcıların şifrelerini kolayca yakalayabilir.
* Blue Team (savunma tarafı) için bu saldırı türünü anlamak çok önemlidir, çünkü önlem alabilmek için tehdidi bilmek gerekir.

**4. Nasıl Kurulur? (Kali Linux örneği)**

Responder genellikle Kali Linux gibi pentest dağıtımlarında yüklü gelir. Ama manuel kurulum şu şekilde olur:

1. GitHub’tan indir:

**git clone** [**https://github.com/lgandx/Responder.git**](https://github.com/lgandx/Responder.git)

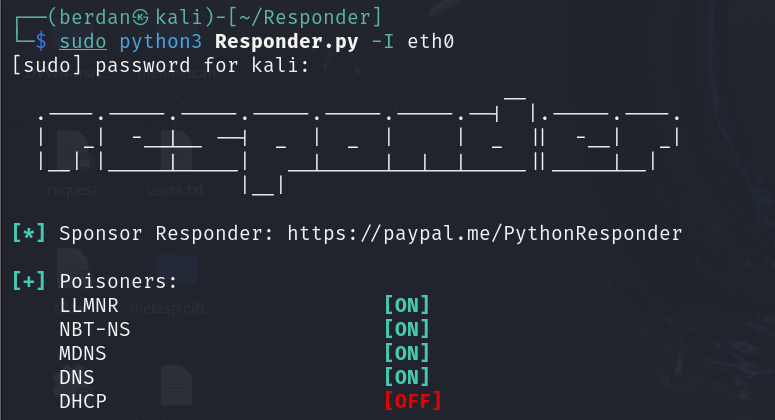
****

**cd Responder**

****

1. Python ile çalıştır:

**sudo python3 Responder.py -I eth0**

****

**eth0** senin ağ arabirimin (Wi-Fi veya Ethernet), bunu **ifconfig** ile öğrenebilirsin.

**5. Örnek Bir Anlatım:**

Diyelim ki bir okul ağına bağlısın. Öğrenciler paylaşımlı bir yazıcıya erişmek istiyor ama yazıcının adı yanlış girilmiş.

1. Bilgisayarlar “bu yazıcı nerede?” diye ağı tarar.
2. Responder hemen ortaya atılır:  
   “Ben o yazıcıyım!” der.
3. Bilgisayar, yazıcıya erişmek için kimlik bilgisi gönderir.
4. Responder bu şifreleri (hash formatında) yakalar ve kaydeder.

Hash dosyası daha sonra kırılırsa, **şifrenin kendisi ortaya çıkar.**