**🕵️‍♂️ Girilen Web Sitelerini Loglama (Ağ Trafiği İzleme)**

**🔍 Konunun Amacı**

Bu uygulamanın amacı; bir ağdaki cihazların ziyaret ettiği web sitelerinin nasıl tespit edileceğini göstermektir.

Bunu yaparken:

* Gerçek zamanlı ağ trafiği izlenecek,
* DNS sorguları veya HTTP istekleri analiz edilecek,
* Hedefin ziyaret ettiği web siteleri **loglanacaktır.**

**🛠️ Kullanılabilecek Araçlar**

Aşağıdaki araçlar eğitim ortamı için uygundur:

**✅ 1. Wireshark**

* Ağdaki tüm paketleri analiz eder.
* DNS, HTTP gibi protokoller filtrelenerek hangi sitelere erişim sağlandığı izlenebilir.

**✅ 2. tcpdump**

* Komut satırından ağ trafiğini kaydeder.
* Filtrelerle sadece DNS veya HTTP paketleri yakalanabilir.

**✅ 3. urlsnarf (dsniff paketiyle birlikte gelir)**

* HTTP trafiğinden ziyaret edilen URL'leri anlık olarak listeler.
* Basit ama etkili bir araçtır.

🌸 **Kurulum (Kali Linux için)**

bash

KopyalaDüzenle

sudo apt-get update

sudo apt-get install dsniff

sudo apt-get install wireshark

🔹 **Yöntem 1: Wireshark ile İzleme**

1. Wireshark’ı açın ve aktif ağ arayüzünü seçin (örneğin wlan0).
2. Filtre olarak aşağıdakilerden biri kullanılabilir:

dns

Hedef cihazın hangi alan adlarına sorgu yaptığını gösterir.

http.request

Ziyaret edilen tam URL’leri görebilirsiniz (HTTPS hariç).

1. İlgili paketlerin içeriğinde Host: başlığı altında hedef siteler görüntülenebilir.

🔹 **Yöntem 2: urlsnarf ile Otomatik Loglama**

urlsnarf -i wlan0

Bu komutla, HTTP üzerinden gidilen URL’ler terminalde şu şekilde listelenir:

GET http://www.instagram.com/ HTTP/1.1

GET http://www.haberler.com/ HTTP/1.1

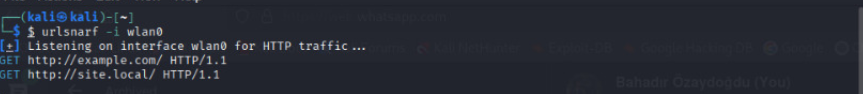
⚠️ Not: HTTPS sitelerde içerik şifreli olduğu için urlsnarf çalışmaz.

🔹 **Yöntem 3: tcpdump ile DNS Loglama**

tcpdump -i wlan0 port 53

Bu komut, DNS sorgularını anlık olarak yakalar:

192.168.1.15.53245 > 8.8.8.8: 12345+ A? facebook.com. (29)



**🧪 Uygulama Senaryosu (Sınıf İçin)**

1. Öğrenciler aynı ağda olacak şekilde konumlandırılır.
2. Bir cihaz hedef, diğeri dinleyici olarak belirlenir.
3. Yukarıdaki araçlardan biri ile trafik izlenir.
4. Öğrenciler ziyaret edilen siteleri **anlık olarak** gözlemler.
5. HTTPS siteler için DNS trafiği yorumlanır (tam URL değil, alan adı görünür).

**🎯 Sonuç**

Bu uygulama sayesinde öğrenciler:

* Web trafiğinin nasıl işlendiğini,
* DNS ve HTTP protokolünün temel mantığını,
* HTTPS'in neden gerekli olduğunu öğrenirler.

Ayrıca saldırganların hangi yöntemlerle bilgi toplayabileceğini ve bunu engellemenin yollarını fark ederler.