**DİNLME / SNIFF ARAÇLARI**

**Sniffing (Dinleme) Nedir?**

Sniffing, ağ üzerindeki veri paketlerinin izinsiz olarak dinlenmesi ve analiz edilmesi işlemidir. Genellikle saldırganlar, hedef sistem ile dış dünya arasındaki iletişimi izlemek, oturum bilgisi veya kimlik bilgileri gibi hassas verileri ele geçirmek amacıyla kullanır. Bu süreçte kullanılan araçlar, ağdaki zayıflıkları ortaya çıkarabilir veya erişim elde etmek için köprü görevi görebilir.

**Kullanım Alanları:**

✓Ağ trafiğini analiz etmek

✓Kimlik bilgisi yakalama (credentials harvesting)

✓HTTPS downgrade gibi saldırılar

✓MITM (Man-in-the-Middle) saldırılarını gerçekleştirme

✓Port yönlendirme ve trafik manipülasyonu

✓VPN tünelleri oluşturma

**Popüler Sniffing Araçları**:

**1**. Bettercap

**2.** Interactsh

**3**. Ligolo-ng

**ARAÇ 1: BETTERCAP**

**Bettercap Nedir:**

Bettercap, ağ trafiğini izlemek, manipüle etmek ve saldırılar gerçekleştirmek için kullanılan çok yönlü ve güçlü bir MITM (Man-in-the-Middle) aracıdır. HTTP, HTTPS, DNS, TCP, UDP gibi pek çok protokolü dinleyebilir. Ağ saldırıları, paket manipülasyonu ve parola yakalama gibi birçok özelliğe sahiptir.

**Özellikleri:**

✓Ağ taraması (network discovery)

✓Paket dinleme ve manipülasyonu

✓DNS spoofing, ARP spoofing, ICMP redirect

✓HTTP(S) proxy, credential sniffer

✓Web oturumu ele geçirme (session hijacking)

✓Modüler yapı: script ve modül desteği

✓CLI (komut satırı) üzerinden kontrol

**Kullanım Alanları**:

•Red Team testlerinde ağ manipülasyonu

•Kimlik bilgisi toplama

•Şifreli trafik analizi (downgrade yapılırsa)

•DNS yönlendirme saldırıları

•Yerel ağ güvenlik zafiyeti tespiti

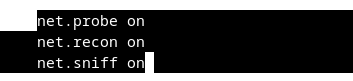
•MITM saldırıları ve eğitim amaçlı analizler

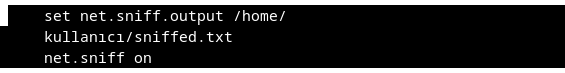
**Kurulum Aşamaları:**

**1. Bettercap’i Kurmak: **

**2. Kullanım Başlatmak: **

**3. Modül Yüklemek (Örnek):**

****

**4. HTTP Kullanıcı Bilgisi Yakalama Örneği: **

**Dikkat Edilmesi Gerekenler:**

✓HTTPS trafiğini analiz etmek için sertifika veya downgrade gerekebilir

✓ARP spoofing işlemleri hedef sistemlerde alarm tetikleyebilir

✓Kendi ağınız dışında kullanımı etik ve yasal değildir

✓Ağda kullanılan güvenlik önlemleri aracı engelleyebilir veya loglayabilir

**ARAÇ 2: INTERACTSH**

**Interactsh Nedir:**

Interactsh, güvenlik araştırmacıları ve Red Team uzmanları tarafından kullanılan, etkileşimli güvenlik testi aracıdır. Özellikle out-of-band (OOB) saldırılar için geliştirilmiştir. Hedef sistemde DNS, HTTP, HTTPS gibi dış istekleri tetikleyip, bu istekleri dinleyerek zafiyet varlığını doğrular.

**Özellikleri:**

✓Out-of-Band (OOB) saldırıları algılar

✓DNS, HTTP, HTTPS, SMTP gibi protokolleri dinler

✓Gerçek zamanlı geri dönüş sağlar

✓Otomatik payload oluşturur

✓API ve CLI desteği mevcuttur

✓Zafiyetlerin sessizce tespiti için idealdir

**Kullanım Alanları:**

•SSRF (Server-Side Request Forgery)

•RCE (Remote Code Execution)

•Blind XSS / Blind SQLi tespiti

•Log4Shell gibi OOB saldırı vektörleri

•Red Team testlerinde gizli izleme

•Güvenlik açığı doğrulama

**Kurulum Aşamaları:**

**1. Go Kurulumu (Gerekirse): **

**2. Interactsh Client’ın Kurulması: **

**3. Kullanımı Başlatmak: **

**4. Bir Payload ile Kullanım Örneği:**

-Bir XSS payload’una Interactsh domain’i gömülerek çalıştırıldığında, hedefin dışarıya yaptığı isteği Interactsh algılar.

**Dikkat Edilmesi Gerekenler:**

✓Genellikle hedef sunucunun dış dünya ile bağlantısı olması gerekir

✓DNS ve HTTP kayıtları hassas bilgi içerebilir

✓Test edilen sistemde iz bırakmadan zafiyet testi yapılabilir

✓Yanlış yapılandırıldığında sonuç alınamayabilir.

**ARAÇ 3: LIGOLO-NG**

**Ligolo-ng Nedir:**

Ligolo-ng, güvenli ve şifreli bir şekilde reverse shell (ters bağlantı) tüneli kurmak için kullanılan modern bir proxy / tunneling aracıdır. Genellikle, hedef sistem ile Red Team operatörü arasında bir bağlantı kanalı oluşturmak için tercih edilir. VPN benzeri bir yapı sunar.

**Özellikleri:**

✓TLS (şifreli) tünelleme desteği

✓SOCKS ve TCP tünelleme

✓Çoklu istemci bağlantısı

✓Yüksek performanslı ve güvenli iletişim

✓Proxy-chaining destekler

✓Kolay kurulum ve kullanım

✓Linux, Windows ve macOS desteği

**Kullanım Alanları:**

•Red Team operasyonlarında iç ağa sızdıktan sonra güvenli bağlantı kurma

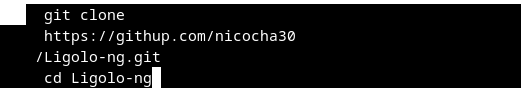
•Ağ pivoting (bir sistem üzerinden diğerlerine atlama)

•Güvenli ters bağlantı tünelleri

•Şifreli shell ve port yönlendirme

•Sızma testi sonrası veri aktarımı ve erişim devamı

**Kurulum Aşamaları (Linux – Operatör tarafı):**

**1. Ligolo-ng deposunun klonlanması: **

**2. Binary dosyalarının derlenmesi: **

**3. Agent ve Proxy çalıştırma:**

-Önce operatör tarafında proxy başlatılır: 

-Sonra hedef sisteme agent gönderilir ve bağlantı sağlanır: 

**Dikkat Edilmesi Gerekenler:**

✓Hedef sistemde outbound bağlantılar engellenmemelidir

✓TLS sertifikaları düzgün yapılandırılmalı veya -selfcert ile geçici sertifika kullanılmalı

✓Kullanım sonrası bağlantılar düzgünce kapatılmalıdır

✓Hedef sistemde çalıştırılacak agent fark edilmemeli (antivirüs önlemi)