AĞ İÇİ PENTEST YÖNTEMLERİ VE SOSYAL MÜHENDİSLİK

Sunan: Şeyma ATMACA

Bugünün Konuları

Kısaca ana hatlar

Penetration Test nedir ?

Günümüzde Bazı Sızma(Pentest) Testleri

Sızma Testi Adımları

Ağ İçi Saldırı Yöntemleri

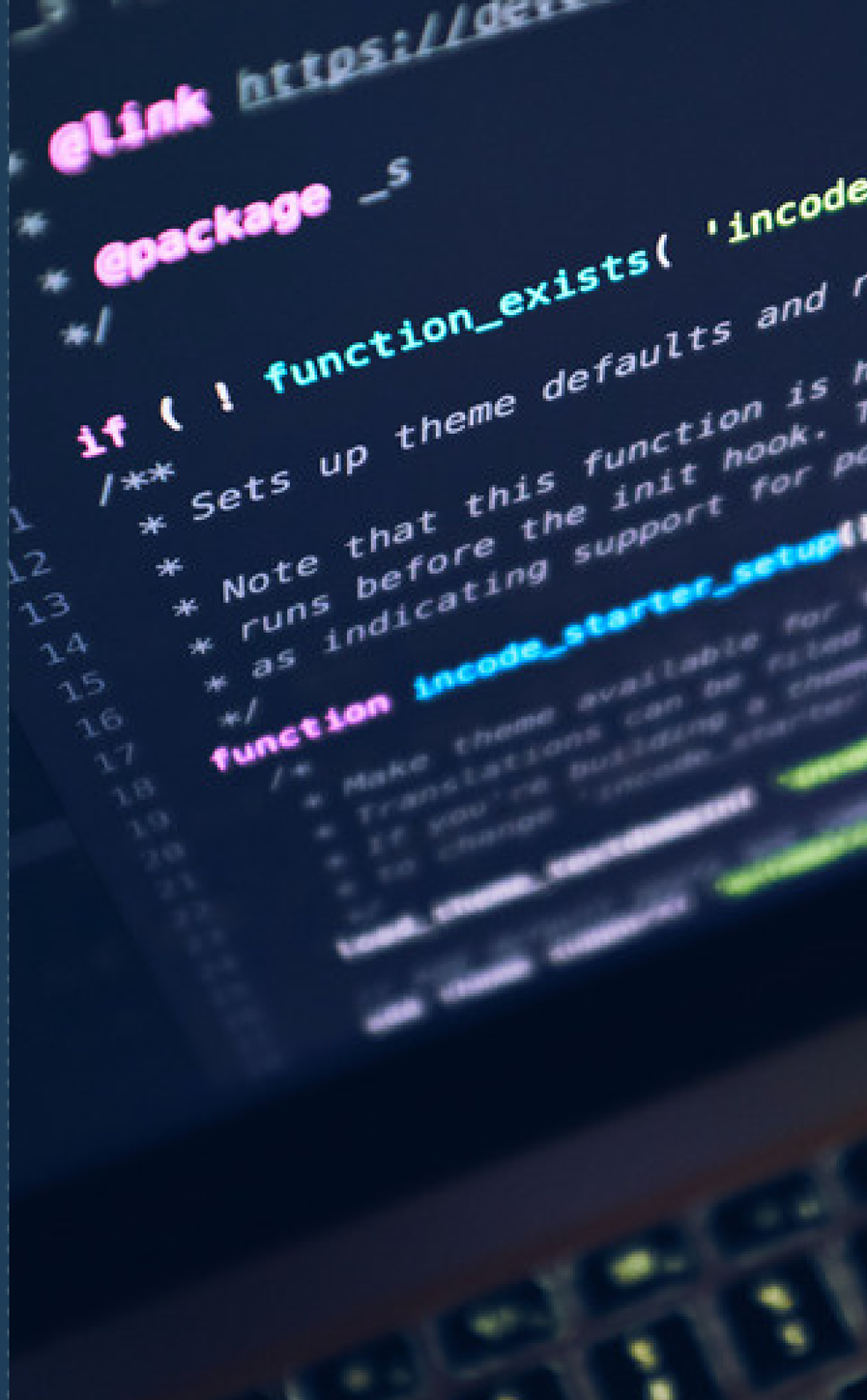
Sosyal Mühendislik Nedir

Neden Sosyal Mühendislik

Sosyal Mühendislik Yöntemleri

Penetration Test

Kelime anlamı olarak "Sızma testi" denilebilir. Amaç herhangi bir sistemde var olan açığı bulmak, bulunan açıkları sömürmek ve son olarak rapor oluşturmaktır.



Sızma testini yapan kişi,

bir saldırganın gözünden sistemdeki açıkları bulur ve bu noktalardan saldırı gerçekleştirir. Yani saldırgan gibi davranıp önceden önlem alma süreci diyebiliriz.

Günümüzde Bazı Sızma Testleri

NETWORK SIZMA TESTLERİ

Hedef ağ ve üzerindeki sistemlere yönelik sızma testleridir.

WEB UYGULAMA SIZMA TESTLERİ

Yetkili kullanıcı profilleri, uygulama mantık hataları, girdi noktaları ve fonksiyonlarının testidir.

SOSYAL MÜHENDİSLİK SIZMA TESTLERİ

Kullanıcı dikkatsizliğinden yaralanmaya dayanır.

MOBİL SIZMA TESTLERİ

Mobil servislere yönelik yöntemleri içerir.

Sızma Testi Adımları

- KEŞİF
- HOST KEŞFİ
- BİLGİ TOPLAMA
- PORT TARAMA
- AĞ ANALİZİ
- VULNERABİLİTY ASSESSMENT
- EXPLOİTİNG
- YETKİ YÜKSELTME
- SİSTEMDE İLERLEME
- RAPORLAMA

SALDIRI ADIMLARI

BİLGİ TOPLAMA

- Sunucu ve servis tarama
- Ağ haritasının çıkarılması
- Ağ servisleri hakkında bilgi toplama

SERVİS VE KULLANICI ANALİZİ

- İşletim sistemi tespiti
- Ağ servisleri ve sistem kullanıcılarının tespiti

GENEL AĞ GÜVENLİĞİ DEĞERLENDİRMESİ

- Ağ segmentasyonu
- Sistem güvenlik konfigürasyonu

ZAFİYET ANALİZİ VE EXPLOİT ETME

- Parola saldırıları
- Servis versiyonlarının sahip olduğu zafiyetlerin tespiti ve test edilmesi

SOSYAL MÜHENDİSLİK NEDİR

Sosyal Mühendislik ;

Hedef kişilerin zafiyetlerini kullanmak suretiyle istenen bilgi veya bilgilerin ele geçirilmesi işlemidir. Mevcut sistem veya servislerin güvenlik seviyesi, insan faktörü olduğu sürece önemli değildir.

SOSYAL MÜHENDİSLİK SALDIRI YÖNTEMLERİ

Omuz Sörfü

Erişim kısıtı olan ortamlarda kurbanın izlenmesi durumudur.

Çöp Karıştırma

Önemsiz görülen belgeler, şirket toplantı takvimlerinin incelenmesi, çöpe atılan diskler, şirket telefon rehberleri, post-it'ler,imla hatasından sebep atılan dokümanlar gibi metaryellerin incelenmesi

Rol Yapma

Saldırganın uygun bir senaryo oluşturması sonucu kurban ile iletişime geçmesi durumudur.

SOSYAL MÜHENDİSLİK SALDIRI TÜRLERİ

Tersine Sosyal Mühendislik

Sabotaj, pazarlama ve destek adımlarından oluşan, kurbanın bizzat kendisinin yardım talep ettiği bir saldırı türüdür.

Oltalama

Genelde e-posta yolu ile birden fazla kişiye yönelik yapılabilen saldrılardır.