AĞ GÜVENLİĞİ VE SIZMA TESTİ

~ cat penetration_testing/introduction.txt

Bilgisayar sistemlerini, ağları veya web uygulamalarını tarayarak sistem üzerindeki zafiyetleri bulmak.

~ eog penetration_testing/Methodology.png

~ cat penetration_testing/planing.txt

→ NDA imzalanması (Gizlilik Sözleşmesi)
→ Test içeriğinin belirlenmesi
→ Sözleşme
→ Sızma testi takımının belirlenmesi

~ cat penetration_testing/recon/passive-scaning.txt

OSINT(OPEN SOURCE INTELLIGENCE)

→ Herkesin erişimine açık kaynakları kullanarak bilgi toplama.

→ Google, Bing…

→ DNS

→ ...

~ cat penetration_testing/recon/passive/search-engine.txt

Google
- → Dork
  - → site:*.ankara.edu.tr
  - → inurl:login site:*.ankara.edu.tr
- → GHDB
  - → exploit-db.com/google-hacking-database/

Bing
- → IP:x.x.x.x

~ cat penetration_testing/recon/passive/DNS.txt

→ dig -x <IP>
→ nslookup <IP>
→ fierce -dns ankara.edu.tr
→ dnsmap ankara.edu.tr
→ dnsdumpster.com
→ ...

~ cat penetration_testing/recon/passive/network.txt

- → ripe.net
  - → Avrupa ip dağıtımı
  - → ASN(Autonomus System Number) Araması
  - → IP block tespiti
  - → Yetkili kişi bilgileri
- → Shodan.io
  - → Arama motoru
  - → Bütün dünyadaki ipleri taratır
  - → Servisleri bulmamıza yarar

~ cat penetration_testing/recon/passive/email.txt

Theharvester

→ Mail,DNS vs bulmaya yarar.

haveibeenpwned.com

→ Verilen E-mail adresinin herhangi bir veri güvenliğini ihlal edip etmediğini kontrol eden bir site.

~ cat penetration_testing/recon/passive/other.txt

FOCA

→ Windows programı

→ Metadata Kontrolü

netcraft.com

→ Hedefin sistemin işletim sistemini öğrenilebilir.

alexa.com

→ Domain'ler hakkında istatiksel bilgiler tutan bir servis.

archive.org :

→ 1996 yılından günümüze kadar açılan bütün web sitelerin indekslerine -hâlihazırda siteler silinmiş bile olsa- ulaşmanız mümkün.

~ cat penetration_testing/recon/passive/other-2.txt

pastebin.com

→ Dump'larınpaylaşıldığı bir site. - site:pastebin.com intext:"password"

tineye.com

→ Görselle arama yapılabilen bir site.

wappalyzer.com

→ İçerik yönetim sistemlerini, e-ticaret platformlarını, web frameworklerini, sunucu yazılımlarını, analiz araçlarını tespit eden eklenti.