**Web Pentest Prosedürü**

**8 Haziran 2025**

**Volkan Güler**

**NMAP, NUCLEİ VE SUBFİNDER YÜKLENMİŞ OLMASINI UNUTMA.**

**1. SUBFINDER ÇALIŞTIR**

Hedef web sitesine ait tüm alt alan adlarını tespit etmek için aşağıdaki komut kullanılır:

subfinder -d hedefsite.com -o subs.txt

Bu komut, subs.txt dosyasına tüm bulunan alt alan adlarını yazar.

**2. ALT ALAN ADLARININ IP KARŞILIĞINI GÖRSEL EDİN**

Subdomain ve karşılık gelen IP adreslerini görümek için:

while read domain; do

ip=$(dig +short "$domain" | grep -E '^[0-9.]+$' | head -n1);

echo "$domain → ${ip:-[Çözülemedi]}";

done < subs.txt

**3. TAM OTOMATİK TARAMA: automated\_web\_scan.sh**

Aşağıdaki script tüm analizleri yapar:

* Subdomain ve IP tabanlı Nmap taraması
* Risk seviyelerine göre sınıflandırma
* nuclei ile CVE & Misconfiguration tespiti

Scripti çalıştırmak için:

chmod +x automated\_web\_scan.sh

./automated\_web\_scan.sh

**4. DIRSEARCH İLE ALT DİZİNLERİ TARA**

Sadece bazı web sitelerini (nmap taramasında online ve 80,443 aktif olanları) manuel tara.

dirsearch -u hedefsite

**4. ÇIKTILARI ANALİZ ET**

Script tamamlandıktan sonra aşağıdaki dosyalar üzerinden analiz yap:

* nmap\_subdomain\_results.txt → Uygulama bazlı Nmap taraması sonuçları
* nmap\_ip\_results.txt → IP/Servis bazlı Nmap taraması sonuçları
* risk\_report.txt → Otomatik risk derecelendirme raporu
* nuclei\_results.txt → CVE ve konfigürasyon zaafiyetleri
* EK OLARAK HER BİRİNE WEB ÜZERİNDEN ERİŞ VE ZAAFİYET KONTROL ET

Bu çıktıları ChatGPT'ye yükleyerek analiz etmesini iste. Aşağıdaki başlıklarda Excel formatında bulgular istemeyi unutma:

| Bulgu Kritiklik Seviyesi | Bulgu Tanımı | Kontrol Tanım(lar)ı | Kurum Yönetimine Bulgu Açıklaması | Açıklamanın Teknik Karşılığı | Nedeni | Etkisi | Düzeltici Öneriler |

Ayrıca versiyon güncellemesi gereken tüm servisleri tespit ettirmeyi unutma.

**---------------------------------------------**

**#!/bin/bash**

**echo "🔍 [1] Subdomain üzerinden Nmap taraması başlıyor..."**

**> nmap\_subdomain\_results.txt**

**while read domain; do**

**if [[ -n "$domain" ]]; then**

**echo "[\*] Taranıyor: $domain"**

**echo "## $domain ##" >> nmap\_subdomain\_results.txt**

**nmap -A -T4 "$domain" >> nmap\_subdomain\_results.txt 2>/dev/null**

**echo -e "\n--------------------------\n" >> nmap\_subdomain\_results.txt**

**fi**

**done < subs.txt**

**echo "✅ Subdomain tarama tamamlandı: nmap\_subdomain\_results.txt"**

**echo "🔍 [2] IP listesi çıkarılıyor..."**

**> unique\_ips.txt**

**while read domain; do**

**ip=$(dig +short "$domain" | grep -E '^[0-9.]+' | head -n1)**

**if [[ -n "$ip" ]]; then**

**echo "$ip"**

**fi**

**done < subs.txt | sort -u > unique\_ips.txt**

**echo "📌 $(wc -l < unique\_ips.txt) adet benzersiz IP bulundu."**

**echo "🔍 [3] IP üzerinden Nmap taraması başlıyor..."**

**> nmap\_ip\_results.txt**

**while read ip; do**

**echo "[\*] IP taranıyor: $ip"**

**echo "## $ip ##" >> nmap\_ip\_results.txt**

**nmap -A -T4 "$ip" >> nmap\_ip\_results.txt 2>/dev/null**

**echo -e "\n--------------------------\n" >> nmap\_ip\_results.txt**

**done < unique\_ips.txt**

**echo "✅ IP tarama tamamlandı: nmap\_ip\_results.txt"**

**echo "🧠 [4] Risk puanlaması hesaplanıyor..."**

**> risk\_report.txt**

**grep "Nmap scan report for" nmap\_ip\_results.txt | while read line; do**

**ip=$(echo "$line" | awk '{print $5}')**

**ports=$(grep -A20 "$line" nmap\_ip\_results.txt | grep "/tcp" | grep open | wc -l)**

**risk="Low"**

**[[ $ports -ge 5 ]] && risk="Medium"**

**[[ $ports -ge 10 ]] && risk="High"**

**echo "$ip --> $ports open ports --> Risk: $risk" >> risk\_report.txt**

**done**

**echo "📄 Risk değerlendirme tamamlandı: risk\_report.txt"**

**echo "🚀 [5] Nuclei ile tarama başlıyor (CVEs & Misconfig)..."**

**> nuclei\_results.txt**

**while read domain; do**

**echo "[\*] Nuclei taranıyor: $domain"**

**nuclei -u "$domain" -severity low,medium,high,critical -tags cves,misconfiguration >> nuclei\_results.txt**

**done < subs.txt**

**echo "✅ Nuclei tarama tamamlandı: nuclei\_results.txt"**