**🧠 1. Nessus Essentials Nedir?**

**Nessus Essentials**, Tenable tarafından geliştirilen popüler zafiyet tarama aracı **Nessus**’un ücretsiz sürümüdür.

* 16 adede kadar IP adresini tarayabilir.
* Ağdaki cihazlar, işletim sistemleri ve uygulamalar üzerindeki bilinen güvenlik açıklarını tespit eder.
* Ayrıntılı raporlar ve çözüm önerileri sunar.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 Zafiyet tespiti | CVE tabanlı güvenlik açıklarını bulur |
| 🧠 Konfigürasyon denetimi | Yanlış yapılandırmaları tespit eder |
| 🛡️ Güvenlik değerlendirmesi | Açık portlar, servisler, protokoller analiz edilir |
| 📊 Raporlama | HTML, CSV, PDF çıktısı sağlar |
| 🔄 Sürekli güncellenen veri tabanı | Yeni çıkan güvenlik açıklarını hızlıca algılar |

**⚙️ 3. Kurulum (Kali / Linux / Windows)**

**✅ 1. Nessus Essentials indirme:**

* https://www.tenable.com/products/nessus/nessus-essentials adresinden işletim sisteminize uygun paketi indirin.

**✅ 2. Linux üzerinde kurulum örneği:**

metin, yazı tipi, ekran görüntüsü, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ 3. Tarayıcıdan erişim:**

* https://localhost:8834 adresine gidin.
* Nessus Essentials lisans anahtarınızı girin (e-posta ile gelir).

**🚀 4. Kullanım Adımları**

**✅ 1. Yeni tarama oluşturma:**

* **New Scan** → tarama türünü seç (örnek: Basic Network Scan).

**✅ 2. Hedefleri belirleme:**

* IP adresi veya domain girilir.

**✅ 3. Tarama ayarlarını yapılandırma:**

* Port aralığı, kimlik doğrulama bilgileri, tarama süresi gibi parametreler belirlenir.

**✅ 4. Tarama başlatma ve izleme:**

* Tarama sırasında açık portlar, zafiyetler ve risk seviyeleri listelenir.

**✅ 5. Raporlama:**

* Tarama tamamlandıktan sonra rapor **High, Medium, Low** risk seviyelerine göre ayrılır.

**📋 5. Örnek Tarama Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 6. Nessus Essentials ile Tespit Edilebilen Açık Türleri**

* 🛠️ Yazılım güvenlik açıkları (CVE bazlı)
* 📦 Eksik güvenlik yamaları
* 🔑 Zayıf şifreler ve varsayılan kimlik bilgileri
* 🔍 Yanlış yapılandırılmış servisler
* 📡 Açık portlar ve protokoller

**🧪 7. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🛡️ Blue Team denetimleri | Ağ güvenlik seviyesini ölçme |
| 🔍 Pentest öncesi keşif | Potansiyel saldırı vektörlerini belirleme |
| 🧠 Uyumluluk testleri | PCI-DSS, HIPAA gibi standartlara uygunluk kontrolü |
| 🧪 Eğitim amaçlı taramalar | Zafiyet tarama pratiği kazanma |

**🎯 8. Öğrenim Kazanımları**

* Ağ ve sistem zafiyet tarama süreçlerini kavrama
* Nessus arayüzü üzerinden tarama yapılandırmayı öğrenme
* Zafiyet raporlarını okuma ve yorumlama becerisi
* CVE tabanlı güvenlik açıklarının tespit yöntemlerini anlama