****

**İSTANBUL GELİŞİM MESLEK YÜKSEKOKULU**

**BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ**

**BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ (İ.Ö) PROGRAMI**

**NESSUS İLE ZAFİYET TARAMASI**

**FİNAL PROJE ÖDEVİ**

**HAZIRLAYAN**

**MUSTAFA YURTALAN-220175094**

**ÖDEV DANIŞMANI**

**Öğr. Gör. Çisem YAŞAR**

**İSTANBUL-2023**

ÖDEV TANITIM FORMU

YAZAR ADI SOYADI : MUSTAFA YURTALAN

ÖDEVİN DİLİ : TÜRKÇE

ÖDEVİN ADI : NESSUS İLE ZAFİYET TARAMASI

BÖLÜM : BİLGİSAYAR TEKNOLOJİLERİ

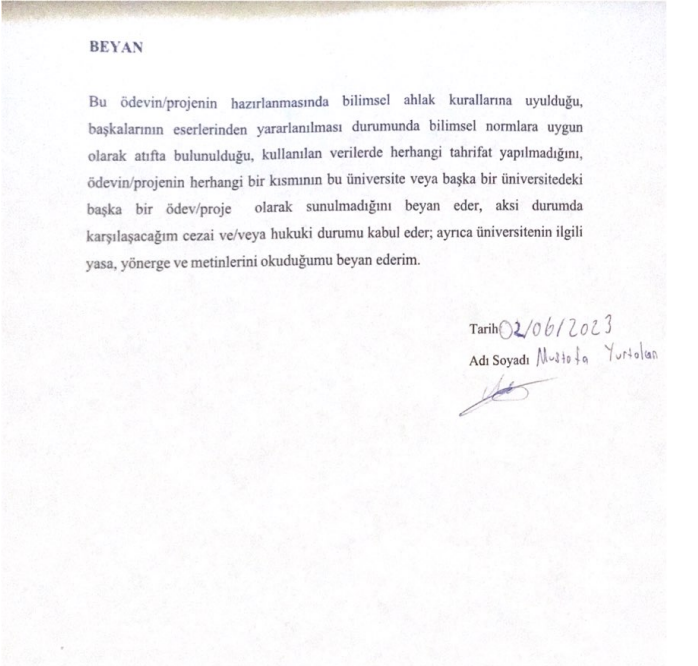
PROGRAM : BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ (İ.Ö)

ÖDEVİN TÜRÜ : FİNAL ÖDEVİN TES. TARİHİ :02/06/2023

SAYFA SAYISI :29

ÖDEV DANIŞMANI : Öğr. Gör.Çisem Yaşar

Beyan



# KABUL VE ONAY SAYFASI

220175094 numaralı Mustafa Yurtalanın’ın Öğrenci Nessus İle Zafiyet Taraması adlı çalışması, benim

tarafımdan Vize/Ders içi/Final ödevi olarak kabul edilmiştir.

Öğretim Görevlisi

Çisem Yaşar

# ÖZET

Nessus, güvenlik alanında kullanılan etkili bir zafiyet tarama aracıdır. Bu araç, sistemlerdeki güvenlik açıklarını ve zafiyetleri tespit etmek için otomatik taramalar gerçekleştirir. Zafiyet taraması, potansiyel zayıf noktaları belirleyerek sistemlerin güvenliğini artırmak için kritik bir adımdır.

Nessus'un temel işlevi, ağ üzerindeki hedef sistemleri taramaktır. Tarama sırasında, sistemlere yönelik bilinen zafiyetleri tespit etmek ve bu zafiyetlerin ciddiyet seviyelerini değerlendirmek için çeşitli teknikler kullanır. Nessus, güncel zafiyet veri tabanına sahip olmasıyla dikkat çeker ve bu veri tabanını kullanarak sistemlerdeki güvenlik açıklarını kontrol eder.

Nessus'un kullanımı oldukça kolaydır ve taranacak hedefleri ve tarama parametrelerini yapılandırmak için bir arayüz sunar. Kullanıcılar, belirli bir ağ veya IP aralığındaki sistemleri tarayabilir, tarama politikalarını özelleştirebilir ve tarama sonuçlarını ayrıntılı bir şekilde inceleyebilir.

Tarama sonuçları, Nessus tarafından oluşturulan ayrıntılı bir rapor şeklinde sunulur. Bu rapor, tespit edilen zafiyetlerin yanı sıra, bunların ciddiyet seviyelerini, etkilenen sistemleri ve önerilen çözümleri içerir. Bu raporlar, sistem yöneticilerine ve güvenlik uzmanlarına, tespit edilen zafiyetleri gidermek ve sistem güvenliğini artırmak için rehberlik sağlar.

Nessus'un güvenlik taramaları sadece bilgisayar ağlarıyla sınırlı değildir, aynı zamanda web uygulamaları ve bulutta barındırılan hizmetler gibi farklı ortamları da tarayabilir. Bu, geniş bir kapsamda zafiyet taraması yapma esnekliği sağlar.

Sonuç olarak, Nessus güvenlik tarama aracı, zafiyetleri tespit etmek ve güvenlik açıklarını ele almak için etkili bir çözümdür.

**Anahtar Kelimeler:** CVSS, Nessus, Pentest, Sistem, Tarama, Zafiyet

# Şekiller Listesi

[Şekil 1https://secromix.com/wp-content/uploads/2021/06/nessuslogo-02.png viii](#_Toc136600609)

[Şekil 2 Tarayıcı da aratma ix](#_Toc136600610)

[Şekil 3 Doğru link ix](#_Toc136600611)

[Şekil 4 Versiyon seçimi ix](#_Toc136600612)

[Şekil 5 Lisans Sözleşmesi ix](#_Toc136600613)

[Şekil 6 Install wizard x](#_Toc136600614)

[Şekil 7 Lisans sözleşmesi x](#_Toc136600615)

[Şekil 8 Klasör seçimi x](#_Toc136600616)

[Şekil 9 Kurulum başlatma onayı xi](#_Toc136600617)

[Şekil 10 Kurulum bitiş ekranı xi](#_Toc136600618)

[Şekil 11 Local host görünümü xi](#_Toc136600619)

[Şekil 12 Welcome to Nessus xii](#_Toc136600620)

[Şekil 13 Nessus varyasyonları xii](#_Toc136600621)

[Şekil 14 Kayıt ekranı xiii](#_Toc136600622)

[Şekil 15 Kullanıcı adı ve parola xiii](#_Toc136600623)

[Şekil 16 Pluginler5J8H-TLKY-4LPN-7ZDW-D55 xiii](#_Toc136600624)

[Şekil 17 Nessusa giriş xiv](#_Toc136600625)

[Şekil 18 Scan arayüzü xiv](file:///C:\Users\MUSTAFA\Desktop\Kişisel%20Güvenlilk%20Teknolojisi.docx#_Toc136600626)

[Şekil 19 My Scans xiv](#_Toc136600627)

[Şekil 20 All Scans xiv](#_Toc136600628)

[Şekil 21 Trash xiv](#_Toc136600629)

[Şekil 22 Policies xv](#_Toc136600630)

[Şekil 23 Plugin Rules xv](#_Toc136600631)

[Şekil 24 Terrascan xv](#_Toc136600632)

[Şekil 25 About xv](#_Toc136600633)

[Şekil 26 Advanced xv](#_Toc136600634)

[Şekil 27 Proxy Server xv](#_Toc136600635)

[Şekil 28 SMTP Server xv](#_Toc136600636)

[Şekil 29 Custom CA xvi](#_Toc136600637)

[Şekil 30 Custom CA xvi](#_Toc136600638)

[Şekil 31 Scanner Health xvi](#_Toc136600639)

[Şekil 32 Notifications xvi](#_Toc136600640)

[Şekil 33 My Account xvi](#_Toc136600641)

[Şekil 34 Politika özelleştirme xvi](#_Toc136600642)

[Şekil 35 Policies xvii](#_Toc136600643)

[Şekil 36 Advandec Scan arayüzü xviii](#_Toc136600644)

[Şekil 37 Gemeral ön izleme xviii](#_Toc136600645)

[Şekil 38 Schedule xviii](#_Toc136600646)

[Şekil 39 Notifications xix](#_Toc136600647)

[Şekil 40 Assesment xix](#_Toc136600648)

[Şekil 41 Malware xx](#_Toc136600649)

[Şekil 42 Hazır halde bir tarama xxi](#_Toc136600650)

[Şekil 43 Tarama Takibi xxi](#_Toc136600651)

[Şekil 44 Tarama Host Ekranı xxii](#_Toc136600652)

[Şekil 45 Vulnerabilities Sayfası xxii](#_Toc136600653)

[Şekil 46 Detaylı zafiyet listesi xxii](#_Toc136600654)

[Şekil 47 Detaylı zafitet xxiii](#_Toc136600655)

[Şekil 48 CVSS Zafiyet sınıflandırması xxiv](#_Toc136600656)

[Şekil 49 Zafiyet Çözümü xxiv](#_Toc136600657)

İçindekiler

[Beyan ii](#_Toc136613702)

[KABUL VE ONAY SAYFASI 3](#_Toc136613703)

[ÖZET 1](#_Toc136613704)

[Şekiller Listesi 2](#_Toc136613705)

[ÖN SÖZ 4](#_Toc136613706)

[GİRİŞ 5](#_Toc136613707)

[1.1 Zaafiyet nedir 6](#_Toc136613708)

[1.2 Pentesting Nedir 6](#_Toc136613709)

[2.1 NESSUS NEDİR 6](#_Toc136613710)

[2.2 Nessus ne için kullanılır 6](#_Toc136613711)

[2.3 Nessus avantajları 7](#_Toc136613712)

[2.4 Nessus kurulumu 7](#_Toc136613713)

[3.1 Nessus arayüzü 13](#_Toc136613714)

[3.2 Scan Arayüzü 13](#_Toc136613715)

[Resources 13](#_Toc136613716)

[Accounts 15](#_Toc136613717)

[4.1 Zafiyet Taraması 15](#_Toc136613718)

[4.2 Taramaya Başlanması 19](#_Toc136613719)

[4.3 Zafiyet Çözümü 22](#_Toc136613720)

[TARAMA İŞLEMİNİ İZLEMEK İÇİN 24](#_Toc136613721)

[Kaynakça 25](#_Toc136613722)

# ÖN SÖZ

“Nessus ile zafiyet taraması” adlı çalışmamda program özelinde bir kullanım kılavuzu oluşturup hakkında yorumlarımı aktarmış bulunuyorum.

Bu çalışmanın gerçekleştirilmesinde destek ve katkılarından dolayı Öğr. Gör. Çisem YAŞAR’e teşekkürlerimi sunarım.

Çalışmam boyunca yanımda olan yakınlarıma bana verdikleri destekten dolayı teşekkür ederim.

Mustafa Yurtalan

# GİRİŞ

Bu ödevde, popüler bir güvenlik tarama aracı olan Nessus'u kullanarak sistemlerdeki potansiyel zafiyetleri taramak ve raporlamak üzerine çalışacağım. Nessus, geniş bir veri tabanına sahip olan ve birçok güvenlik açığına karşı tarayabilen etkili bir araçtır. Bu ödevde, Nessus programını kurma, yapılandırma, hedef sistemlerin taramasını yapma ve elde edilen sonuçları analiz etme süreçlerini ele alacağım.

Nessus programını kullanarak zafiyet taraması yapmak için aşağıdaki adımları izleyeceğim:

1. Nessus programını indirip kuracağım.
2. Kurulum sonrası programı yapılandıracağım ve güncellemeleri kontrol edeceğim.
3. Tarama yapmak istediğim hedef sistemleri belirleyeceğim ve tarama politikalarını tanımlayacağım.
4. Nessus'u kullanarak hedef sistemlerin taramasını gerçekleştireceğim ve taranan zafiyetleri raporlayacağım.
5. Elde edilen raporları analiz ederek, kritik zafiyetleri ve önerilen düzeltme yöntemlerini belirleyeceğim.

Bu ödevde, Nessus programını kullanarak sistemlerdeki zafiyetleri taramak ve güvenlik açıklarını belirlemek için pratik becerilerimi geliştirmeyi hedefliyorum. Nessus'un güvenlik testleri, raporlama yetenekleri ve kullanım kolaylığına odaklanarak, sistemin güvenliğini iyileştirme ve önleyici tedbirler alma konusunda daha bilinçli olmayı umuyorum.

## 1.1 Zaafiyet nedir

Zafiyet kelime anlamınca arıklık, zayıflık anlamına gelir siber güvenlik alanında ise zafiyet bir sistem üzerinde tespit edilen arka kapılar, saldırıya açık olan yerler ve bunlara açık olan yerlerin tamamına verilen addır.

## 1.2 Pentesting Nedir

Pentestingin Türkçe anlamı “Zafiyet Taraması” olarak ifade edilir Zafiyet taraması ile var olan sistemlerdeki çeşitli açıklar bulunup bu zafiyetler üzerinden sistem zarar görmeden önce bertaraf edilmesi hedeflenir.

Pentesting yapabilmek için birçok araç kullanılabilir. Başlıca pentesting araçlarını saymak gerekirse bunlara MetaSploit,WireShark,NetSparker,Burpsuite gibi bir çok örnek verilebilir her aracın kendi içinde avantaj,dejavantaj,kullanım farklılıkları olduğu gibi, kullanıcının tercihine ve var olan durumun getirdiği zorunluklara göre seçilecek olan araç değişiklik gösterebilir.

Bu raporda “Nessus” aracı üzerinde bahsettiğimiz işlemler gerçekleştirilecektir.

# 2.1 NESSUS NEDİR

Nessus, dünya çapında birçok kullanıcıya ulaşmış güvenlik açıklarını bulma ve doğrulanmasında kullanılan en çok da sızma testi (pentest) alanında kullanılan bir araçtır. Birden çok versiyona sahip olduğu gibi Cloud, fiziksel ve sanal ortamlarda farklı sürümleri ile daha etkindir.

Günümüz dünyasında bir genellikle korsan grupları güvenlik açıklarını keşfetse de teknolojinin yaygınlaşmasından mütevellit sıradan kullanıcılar bile çeşitli açıkları bilerek veya şans eseri olacak şekilde keşfede bilmektedir bu durumlarda ortaya çıkacak sorunları en aza indirgemek için Nessus ve benzeri ağ denetimi test araçları görevli kişiler tarafınca kullanılır.

## 2.2 Nessus ne için kullanılır

Bilişim kurumlarının sistemlerinin denetlenmesi, zafiyet taramalarının yapılması, bu açıkların kapatılması alanında hizmet veren siber güvenlik kurumlarında bir sızma testi aracı olarak kullanılarak aracı kullanan güvenlikçiye bir hacker gibi düşünerek olası veyahut olmuş saldırılar üzerinden tüm seçenekleri görerek gerçek bir saldırı ile karşılaşıldığında sistemin açıklık barındıran noktalarının onarılmış ve güvenliğin artırılmasını sağlamaktadırlar.

İçerisinde birçok özelliği barındırsa da kolay bir kullanım arayüzü bulunmadığı, kullanımı hakkında yeterli dokümantasyon bulunmadığı vb. Sebeplerden dolayı standart kullanıcı kullanımına uygun bir program olarak görülmez.



Şekil https://secromix.com/wp-content/uploads/2021/06/nessuslogo-02.png

Nessusun sunduğu güvenlik açıkları;

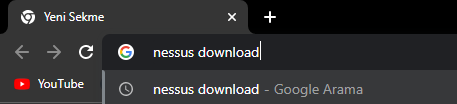
* Verilerin erişilip bunların kontrol edilmesine izin veren zafiyetler,
* Yanlış Kurma sorunlarının önceden bildirilmesi,
* Sistemdeki şifreler ile ilgili zafiyetlerin listelenmesi,
* DDOS saldırılarına açıklık veren TCP/IP sorunlarının görüntülenmesi,
* Hızlı bir şekilde varlık keşfi,
* Yama ve kurulum denetimlerinin yapılması (Güncellemeler),
* Varlık profili çıkartılması,
* Hassas veri keşfi ve bulguların raporlanması,
* Yama (güncelleme, kurulum) yönetimi,
* Çoklu tarayıcı yönetimi ve zafiyet analizi.

## 2.3 Nessus avantajları

* Nessus ile daha büyük ölçekli saldırılara hazırlıklı olunduğu için kurumların saldırı düzeyleri küçülür,
* Kendi içerisinde yüksek hızlı varlık tespiti, zararlı yazılım tespiti özelliklerinin yanı sıra pek çok başka özelliği bünyesinde barındırır,
* Geniş tarama olanakları,
* Saldırıları sınıflandırarak ölçeklendirmede yardımcı olma,
* Dolar bazında düşük maliyet,
* Değişen ve güncellenen saldırı tekniklerine karşı çözüm geliştirme,
* Nessus Home sürümü ile kısıtlı ama ücretsiz hizmete ulaşabilme,
* Kurum ve daha profesyonel kullanımlar için birden çok sürüme ulaşım sağlaması.

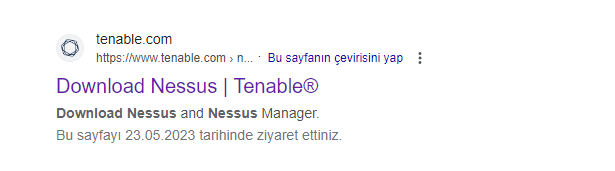
# 2.4 Nessus kurulumu

1. Nessus programını kurabilmemiz için arama motorlarından herhangi birini kullanabiliriz doğru bir arama gerçekleştirebilmek için “Nessus download” kelimeleriyle arama gerçekleştirebiliriz.



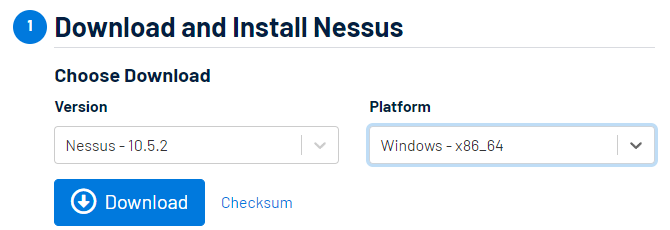
Şekil Tarayıcı da aratma

1. Aratma sonucunda listelenen sitelerden Nessusun yaratıcı şirketi olan Tenable firmasının alakalı linkine girerek işleme devam edilebilir.



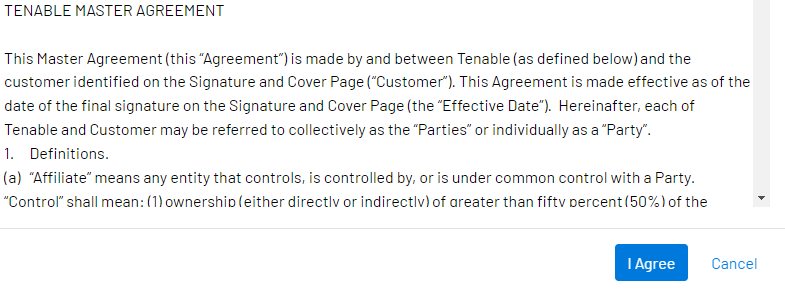
Şekil Doğru link

1. Linke tıkladıktan sonra karşımıza çıkan sayfadan indirmek istediğimiz sürümü “Download” kısmından sisteme uygun olan “Platform” kısmından seçerek kurulum işlemini başlatabiliriz.



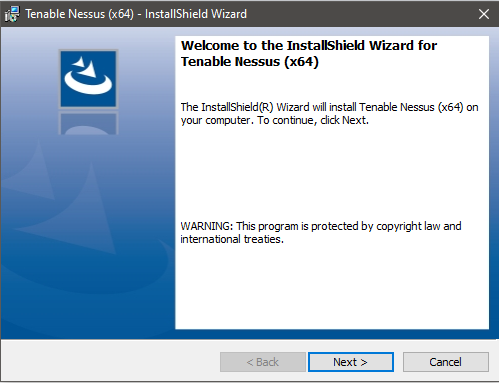
Şekil Versiyon seçimi

1. Download butonuna bastıktan sonra karşımıza çıkan lisans sözleşmesini onaylayalım.



Şekil Lisans Sözleşmesi

I Agree dedikten sonra setup indirilmeye başlayacaktır.

Setup indirildikten sonra üzerine tıklayarak açalım

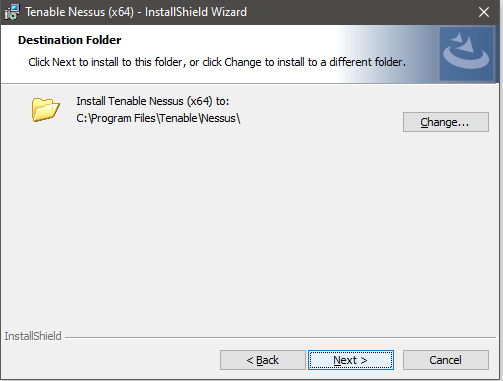
Şekil 6 Install wizard

1. Next tuşuna basarak ilerleyelim karşımıza çıkan lisans sözleşmesini onaylayalım



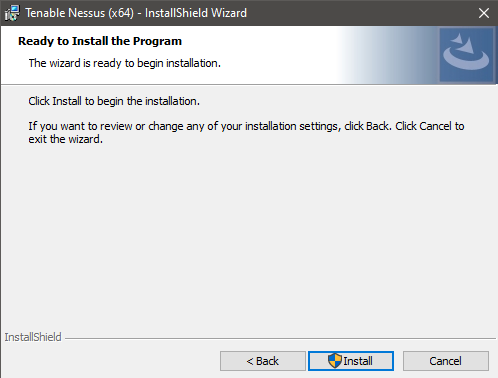
Şekil Lisans sözleşmesi

1. Sözleşmeyi kabul ettikten sonra kurulumun yapılacağı klasörü seçelim

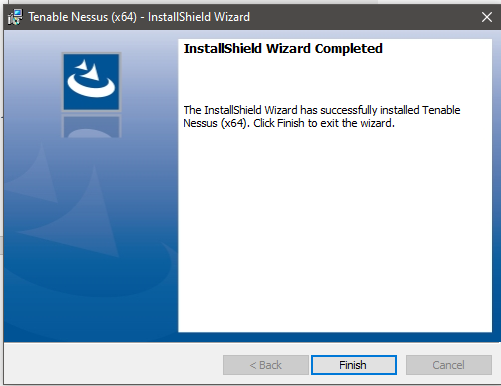


Şekil Klasör seçimi

1. Klasörü seçtikten sonra (Default olarak C klasörüne kuruyor) next diyerek kuruluma başlayalım

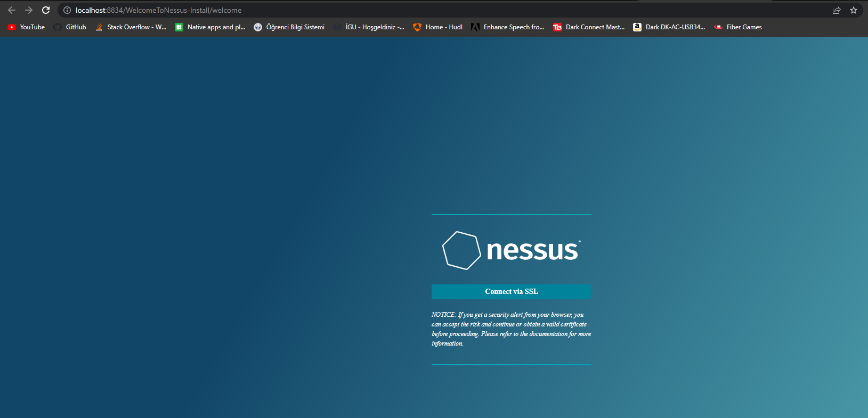


Şekil Kurulum başlatma onayı

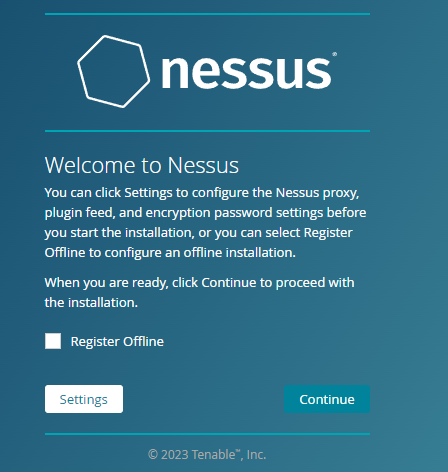
1. Kurulum bittikten Sonra “Finish” Butonuna tıklayarak web sitesine ulaşılır

Şekil Kurulum bitiş ekranı

1. Web sitesine yönlendirildikten sonra local host üzerinden nessusa bağlantı sağlayabilirsiniz bunun için “Connect via SSL” butonuna basıyoruz

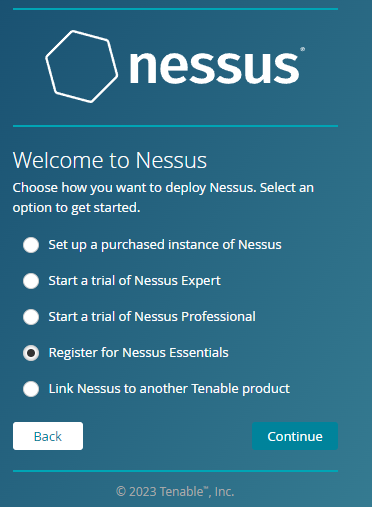


Şekil Local host görünümü

1. Karşımıza çıkan sayfadan istersen nessusa configurasyonlar yapabilir yada devam edebiliriz seçenekleri çıkıyor biz devam etmeyi seçiyoruz

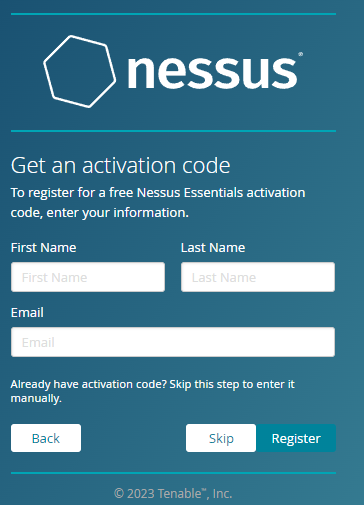
Şekil Welcome to Nessus

1. Çıkan ekran üzerinde bir den fazla nessus varyasyonu olduğu görülmektedir Bunlar her birinin ortak ve farklı işlevleri olmak üzere farklı kullanım alanları için özelleştirilmiş varyasyonlardır raporun devamında “Nessus Essentials” adlı ücretsiz sürüm üzerinden devam edeceğim.



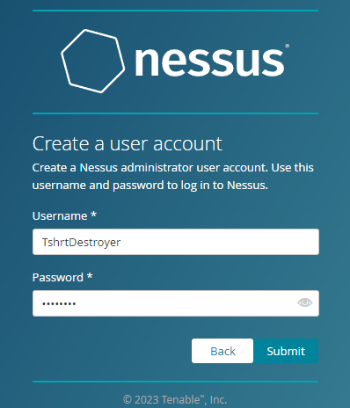
Şekil Nessus varyasyonları

1. Nessus Essantials Varyasyonu kayıt gerektirdiği için ilgi alanları ilgili bilgiler ile doldurup devam ediyoruz.



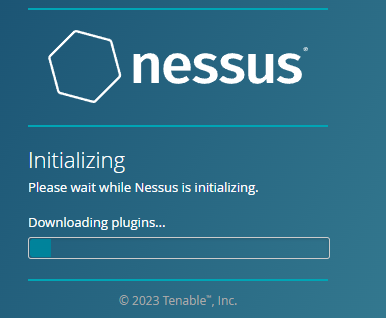
Şekil Kayıt ekranı

1. Alanları doldurduktan sonra bize bir aktivasyon kodu verilecek bu kodu sonra kullanmak için kaydedin ve devam edip bir kullanıcı adı ile parola belirleyin.



Şekil Kullanıcı adı ve parola

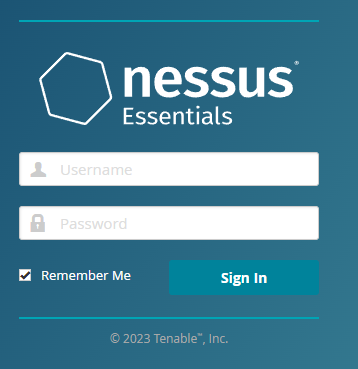
1. Ardından gerekli pluginlerin indirilmesini bekleyin



Şekil Pluginler5J8H-TLKY-4LPN-7ZDW-D55

J8H-TLKY-4LPN-7ZDW-D5FS

1. İndirmeler tamamlandıktan sonra belirlediğimiz kullanıcı adı ve parola ile Nessus uygulamasını kullanmaya başlayabiliriz.



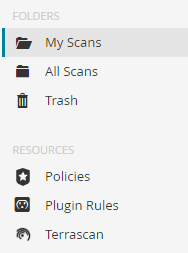
Şekil Nessusa giriş

### 3.1 Nessus arayüzü

Nessun arayüzünü **Scan** ve **Settings** olarak 2 farklı şekilde anlatabiliriz Scan arayüzündeyken taramalar hakkında bilgilere ulaşıp bunları görüntüleyebiliyorken Settings kısmında aracın detaylı ayarlarını manuel bir şekilde değiştirebiliyoruz.

### 3.2 Scan Arayüzü

**Scan** arayüzündeyken folder altında bulunan özellikler;



Şekil Scan arayüzü

1. My Scans: Klasör içerisinde tarama oluşturup var olan taramayı takip etmemize yarar.



Şekil My Scans

1. All Scan: Geçmişte yapılan taramalar dahil bütün taramaların tutulduğu klasördür.



Şekil All Scans

1. Trash: Silinen taramaların depolandığı klasördür.



Şekil Trash

Resources altında bulunan özellikler ise;

1. Policies: Taramalardan önce kalıp şablonlar oluşturup bu şablonları taramalardan önce seçip hazır bir şekilde kullanmaya yarar.



Şekil Policies

1. Plugin Rules: Her hangi bir eklentinin önem derecesini gizlemeye veya değiştirmeye olanak sağlar ayrıca belli sistemlere göre belirli kurallar atanabilir.



Şekil Plugin Rules

1. Terrascan: Statik bir kod altyapısıdır, farklı şekillerde kurulup kullanılabilir.



Şekil Terrascan

Settings kısmına geldiğimizde ise bizi settings ve accounts adlı iki alan karşılıyor bunlardan settings altında;

1. About: Nessusun versiyonu, Lisans kontrolü, gelen güncellemeler gibi bilgilerin görüntülendiği alandır.



Şekil About

1. Advenced: Advenced Settings altında bir çok ayar bulunur manuel bir şekilde aracın üst düzey ayarlarınızı değiştirmenize yarar bilmeden ayarları değiştirmek sorunlara yol açabilir.



Şekil Advanced

1. Poxy Server: Https isteklerini iletmek için kullanılır bu bağlantının bilgileri buradan görüntülenebilir.



Şekil Proxy Server

1. SMTP Server: SMTP Üzerinden belirtilen alıcılara tarama sonuçlarının yollanmasını sağlar filtreler aracılığı ile özel uyarlamalar yapılabilir.



Şekil SMTP Server

1. Custom CA: Pluginlerdeki problemleri bulmaya yarar tarama sırasında bu özelliğe güvenmek doğru olmaz.



Şekil Custom CA

1. Password Mgmt: Çeşitli pasapord parametreleri tanımlamaya ve giriş bilgilendirmelerini ayarlamayı sağlar max giriş denemesi, minimum parola uzunluğu gibi.



Şekil Custom CA

1. Scanner Health: Tarama esnasında ne kadar donanım kullanıldığının yüzdesi bu kullanımların grafik haline getirilmesi bu kısımda bulunur



Şekil Scanner Health

1. Notifications: Nessusun ilk indirildiği andan itibaren hangi tarihte hangi işlemlerin yapıldığının bilgisi listelenir



Şekil Notifications

Accounts altında tek bir özellik bulunur;

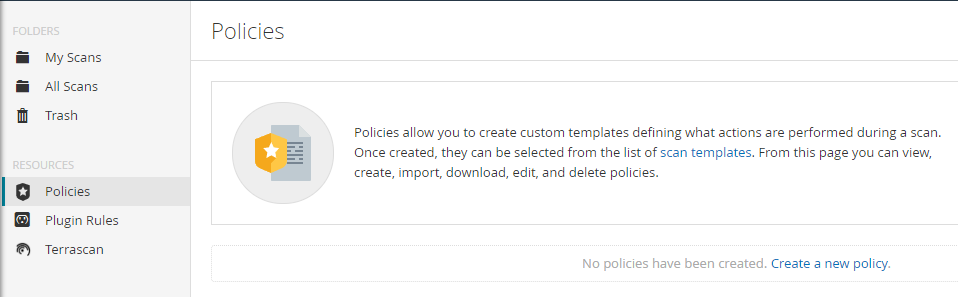
1. My Account: Hesap hakkında kullanıcı adı,email,parola gibi bilgilerin bulunduğu alandır apı keyse de buradan ulaşılabilir ve nessus apisi ile doğrulama yapılabilir



Şekil My Account

### 4.1 Zafiyet Taraması

Nessus, tarama politikaları aracılığıyla hangi güvenlik açıklarının taranacağını ve nasıl taranacağını belirler. İyi bir zaafiyet taraması yapmak için, özelleştirilmiş bir tarama politikası oluşturmanız önemlidir.



Şekil Politika özelleştirme

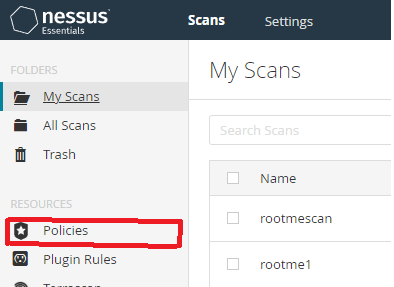
Yönetici arayüzünde, "Policies" (Politikalar) bölümüne gidin ve yeni bir politika oluşturun. Politikanızı adlandırın ve açıklamaları ekleyin. Ardından, politikayı özelleştirmek için gerekli ayarları yapabilirsiniz. Bu ayarlar, taramanın kapsamını, taranacak protokolleri, taranacak portları, taranan güvenlik kontrol noktalarını ve diğer tarama seçeneklerini içerir.

Bu seçenekler içerisinde. Basit bir ağ taraması yapmaktan işlemci bypass taramalarına kadar, birçok seçenek bulunmaktadır.

Kullanılan Nessus versiyonuna göre tüm özelliklere erişim sağlanılamayabilir. Versiyon yükselterek, Nessusun tüm özelliklerine erişim sağlayabilirsiniz.

Nessus ile zafiyet taraması gerçekleştirmek için sırası ile şu adımlar gerçekleştirilebilir.

1. Scans sayfasında Resources altında bulunan “Policies” sekmesine gelinir

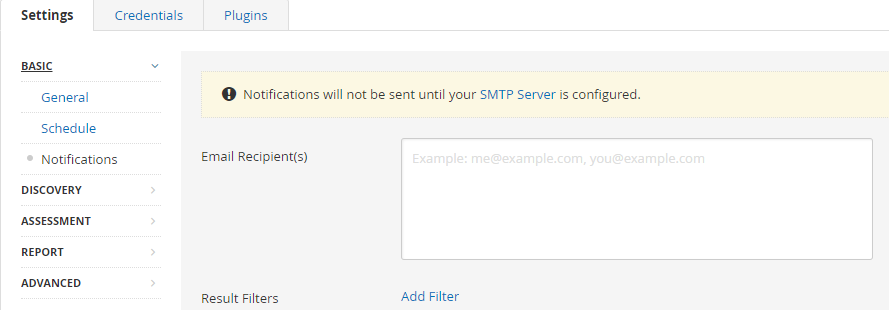


Şekil Policies

1. Policies sayfasında daha önce oluşturulan tarama taslaklarını görüntüleyebilir. Ve bunların arasına yeni taslaklar ekleyebiliriz. Scan templates’e tıkladıktan sonra karşımıza çıkan sayfadan Scanner altından hazır tarama ve zafiyet bulma işlemlerinden birini seçebilir veyahut ta spesifik bir işlem için “User Defined” sayfasından yeni bir taslak oluşturabilir yada var olan bir taslağı kullanabiliriz.

Vulnerabilities altında bulunan “Advanced Scan” e tıklayarak işleme devam edebiliriz

1. Karşımıza gelen sayfada bizi 3 adet kısım karşılıyor Settings,Credentials ve Plugins

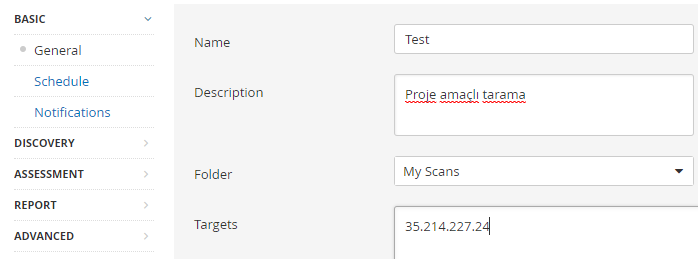


Şekil Advandec Scan arayüzü

Sırası ile açıklamak gerekirse:

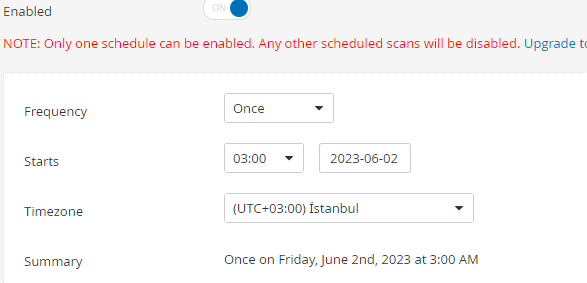
* **Settings:** Tüm ayarların bulunduğu kısımdır kendi altında Basic, Dıscovery,Assesment,Report ve Advanced olarak 5’e ayrılır.

Basic sekmesi altında General,Schedule ve Notifications adlı 3 alan bulunur General sekmesinde Taramamıza bir ad tanımlayabilir Açıklama yazık hedef dosyasını belirtebilir ve hedef IP yapılandırması yapabiliriz



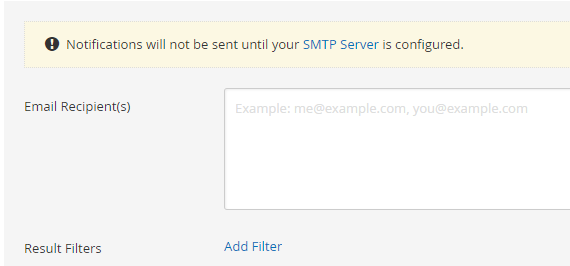
Şekil Gemeral ön izleme

Schedule ile taramamızı zamanlayabiliriz bunu yaparken belli saat aralıkları verip başlangıcını ayarlamak bizim elimizdedir.



Şekil Schedule

Notifications ile eğer ki bir SMTP serveri bağlandıysa hedef bir e-maile tarama sonuçlarını aktarmamızı sağlar.

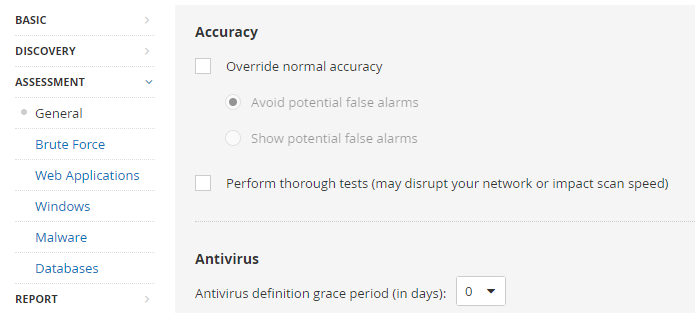


Şekil Notifications

Dıscovery altında birçok yararlı özellik bulunur bu ayarlar genel olarak tarama genişliği ile alakalıdır kaç portun taranacağı, hangi hostların keşfedileceği gibi ayarları bura ile yapabiliriz.

Service discovery en yaygın olarak kullanılan alt özelliğidir buradan TCP portları arasında seçimler yapabiliriz.

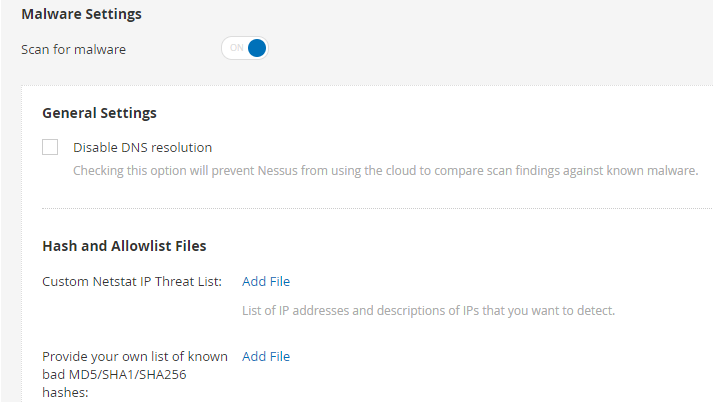
Assesment kısmı Discoveryin aksine saldırı odaklı ayarlamaları yapabiliriz.



Şekil Assesment

Brute Force saldırıların sıklıklarını özelleştirebilir çeşitli işletim sistemlerine spesifik konfigürasyonları buradan ayarlayıp saldırımıza derinlik katabiliriz.

Saldırı amaçlı kullanım dışında Malware özelliği sayesinde bu esnada sistemdeki virüsleri de tarayabilirsiniz.



Şekil Malware

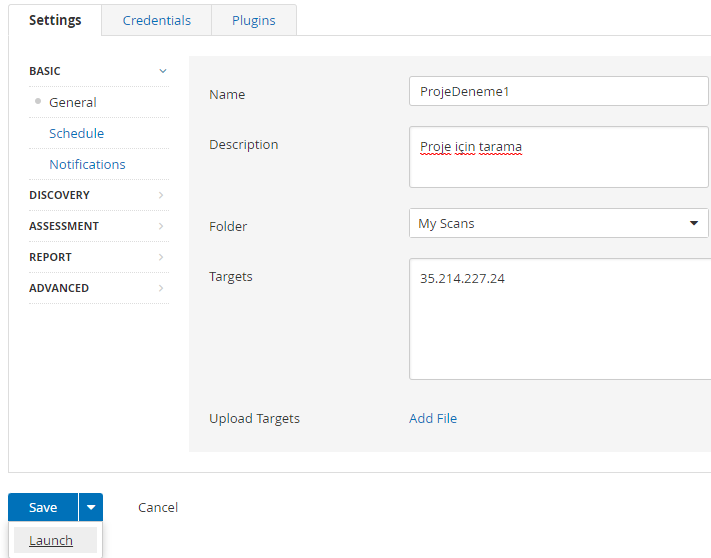
Report Sekmesi ile tarama sonucunda kimlere nelerin raporunun gideceğini özelleştirebiliriz.

Advanced sekmesi Taramanın performansıyla, ilişkili ayarların bulunduğu kısımdır max kaç hostun kaç saniyede aranacağı,saniyede kaç TCP oturumu olacağı gibi standart kullanıcıya lazım olmayan profesyonellere uygun ayarlar vardır.

* **Credentials:** Taramanın Kimlik bilgilerinin olduğu kısımdır host olarak mı API Gateway üzerinden mi yapacağı gibi ayarlar buradan yapılabilir
* **Plugins:** Tüm eklentilerin yapıldığı alandır nessus da taramanız için eksik, gördüğünüz tooları buradan temin edebilir taramanıza ekleyebilirsiniz.

### 4.2 Taramaya Başlanması

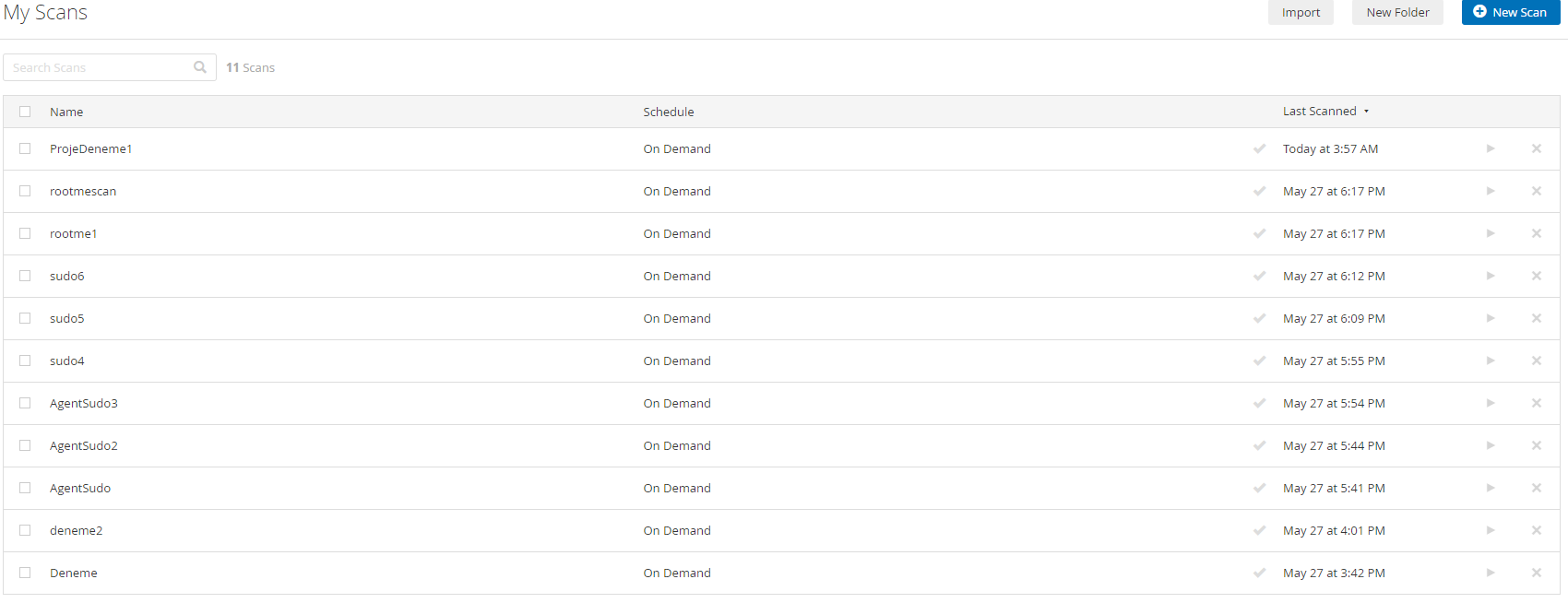
Taramamıza başlamak için Scans>Policies>Advanced Scan dedikten sonra karşımıza çıkan ekrandan taramamıza Ad girmemiz gerekiyor. Devamında isteğe bağlı olarak Descriptiona bir açıklama ekleyebilirsiniz zorunlu bir alan değildir , folder altında taramanın kaydedileceği klasör bulunur Default olarak MyScans tanımlıdır. Targets kısmında hedef IP aderesi Tanımlanır ve sol altta bulunan Launch butonu ile tarama gerçekleştirilmeye başlanır.



Şekil Hazır halde bir tarama

Launch dedikten sonra taramanın gidişatını MyScans sayfası üzerinden takip edebiliriz bu sayfada taramamızın ad bilgisi, takvimlediği zaman, en son ne zaman tarandığı bilgileri bulunur.

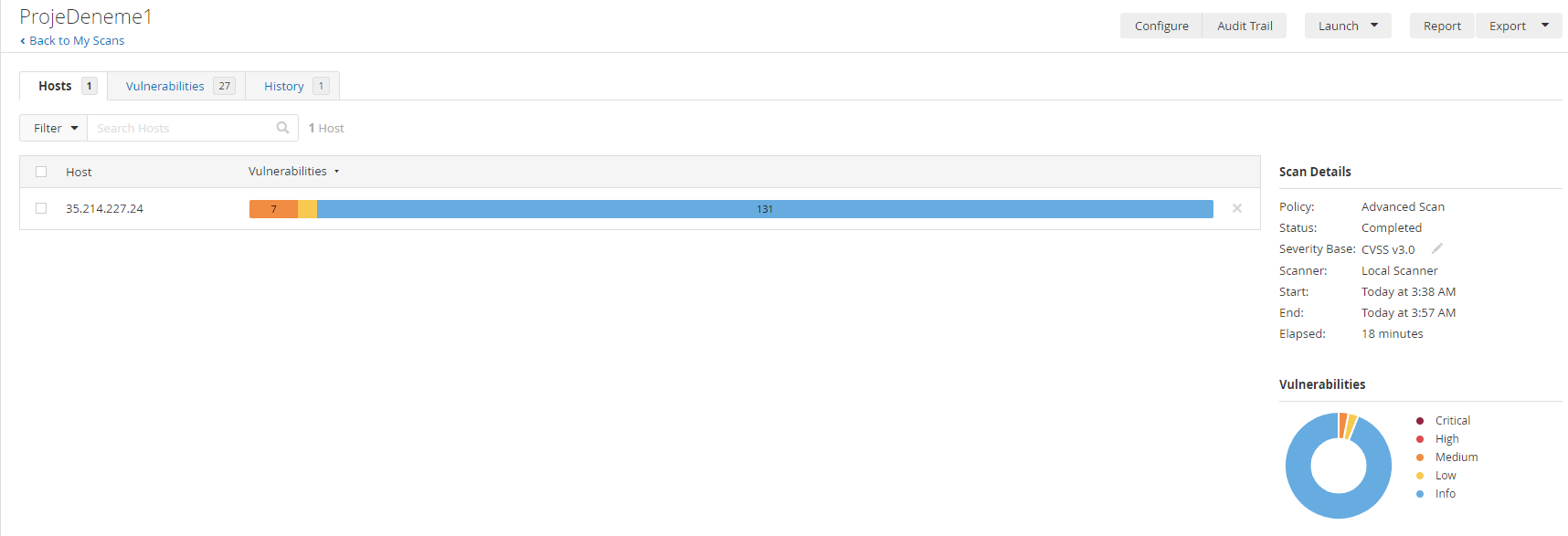
Hemen yanında bulunana üçgen ile taramayı tekrar başlatabilir x ile klasörden silebilirsiniz



Şekil Tarama Takibi

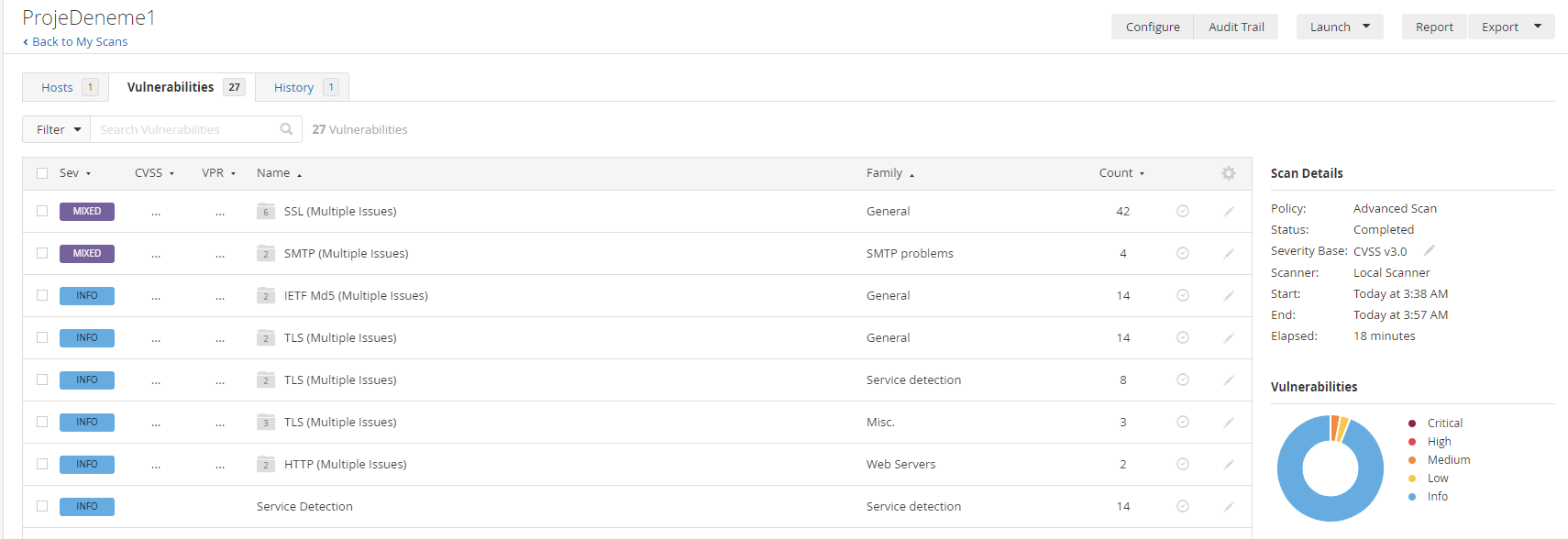
Taramamız tamamlandıktan sonra takvimlenmenin karşısına bir tik işareti çıkacak bu taramanın bittiği anlamına gelir bu süreçten sonra tarama dosyasına girerek zafiyetleri görebiliriz. Tarama süresi tamamen değişken olup oluşturduğunuz poliçeler ile alakalıdır basit bir port taraması 5-6 dk sürebiliyorken, 65535 adet portu taramak istediğimiz de bu süreç saatleri bulabilir.

Taramamıza girdiğimiz de karşımıza çıkan sayfada Hosts,Vulnerabilities ve History kısımlarını görmekteyiz bu sayfalardan Host genel tarama bilgilerini gösterir taramanın poliçesi, statüsü, ne zaman başladığı, ne zaman bittiği, zafiyetlerin grafikte gösterilmesi gibi bilgileri buradan görüntüleyebiliriz.



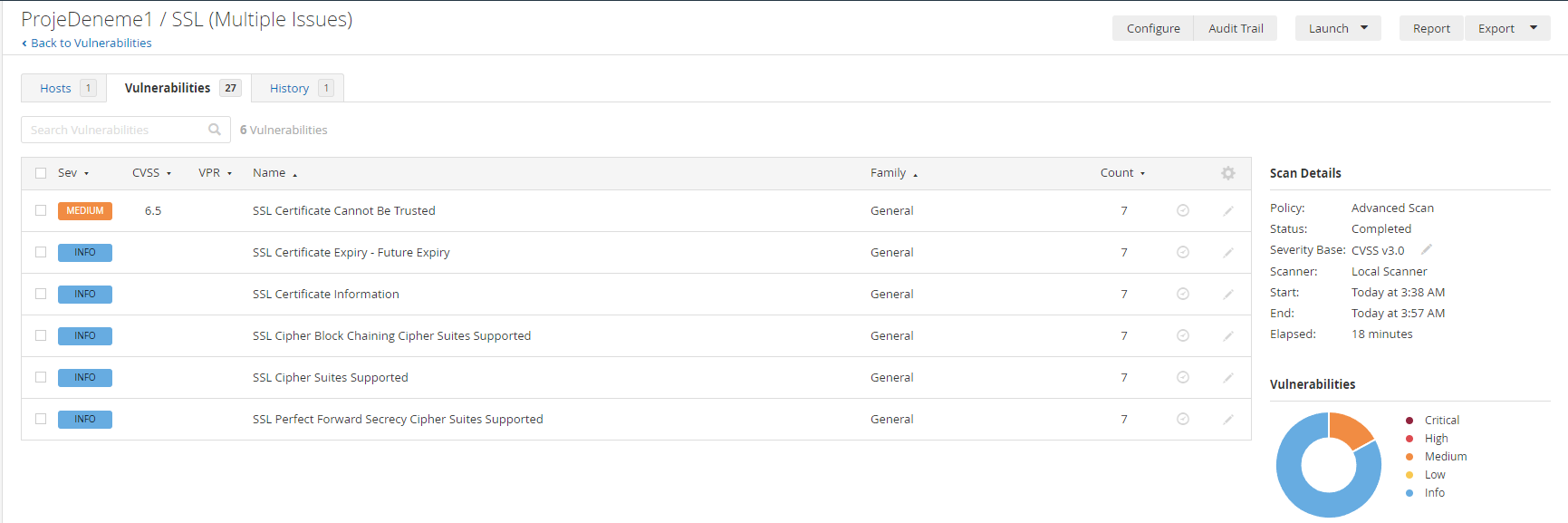
Şekil Tarama Host Ekranı

Vulnerabilities sayfası detaylı bir şekilde zafiyetleri görüntüleyebildiğimiz sayfadır. Bu sayfada zafiyetleri filtreleyebilir, CVSS (Ortak Güvenlik Açığı Puanlama Sistemi) Derecesini görebilir, zafiyetin adını öğrenebilir, bulunduğu familyayı görüp kaç defa sayıldığının bilgilerine ulaşabiliriz.



Şekil Vulnerabilities Sayfası

Listelenen zafiyetlerden birine girdiğimiz de detaylı bir şekilde o zafiyet hakkında bilgiler bizi karşılıyor yine adı, CVSS değeri, familyası gibi genel bilgilerin dışında

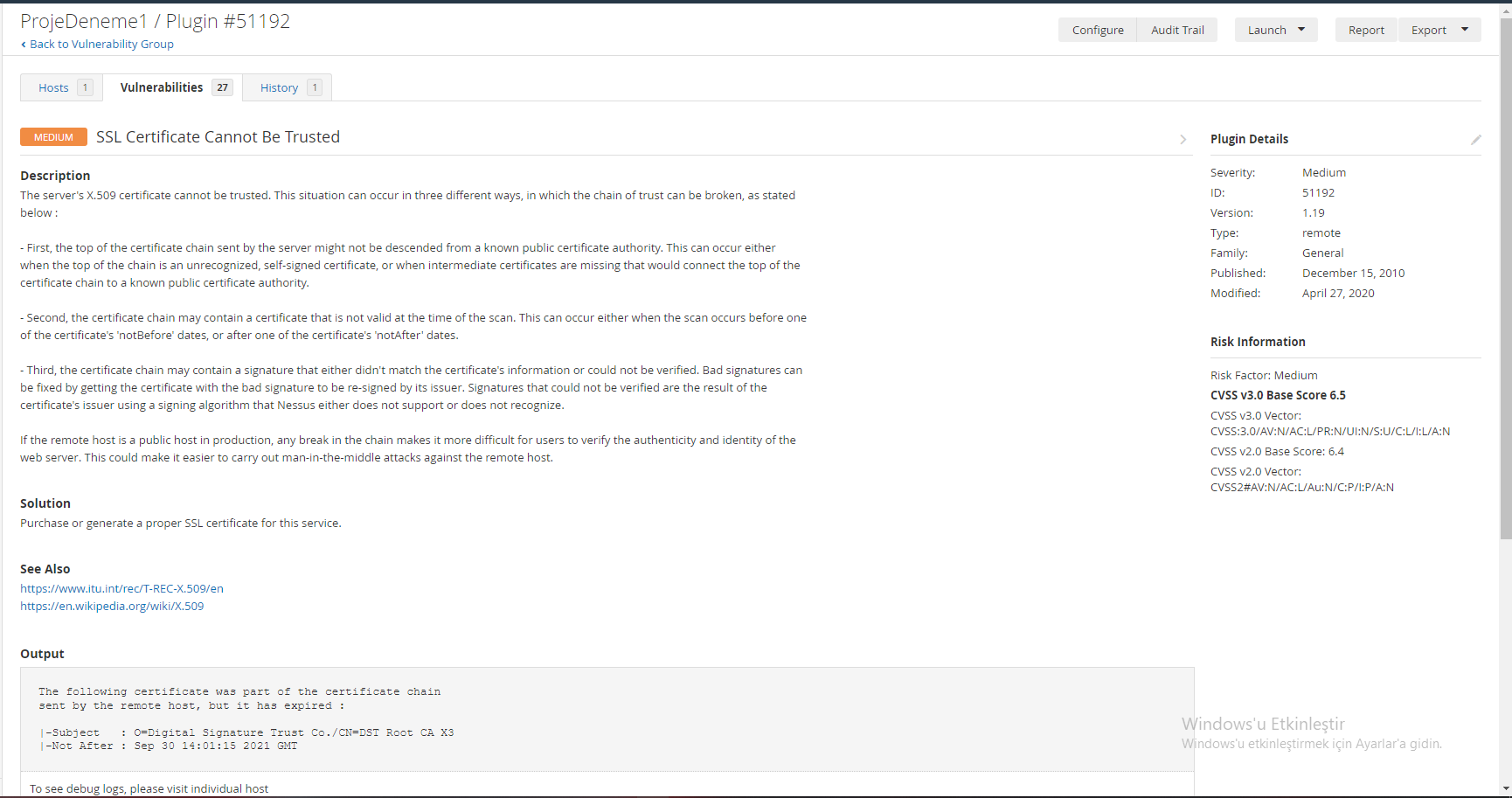


Şekil Detaylı zafiyet listesi

Listede bulunan bir zafiyeti seçtiğimiz de karşımıza bu zafiyetin tanımı, çözümü

Ayrıca bakabileceğimiz kaynaklar, debug log çıktısı ve hangi portlarda görüldüğünün bilgisi verilir.

Nessusun zafiyet taramasındaki en büyük farkı bu bilgileri toplu bir şekilde bize sunması ve hazır rapor olarak bize ulaştırmasıdır.



Şekil Detaylı zafitet

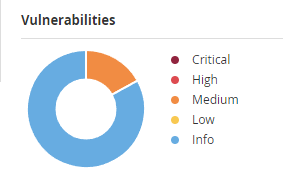
History sayfasından ise daha önce kaç defa bu tarama üzerinde işlem yapıldığı bilgilerini görebilirsiniz.

### 4.3 Zafiyet Çözümü

**CVSS NEDİR**  
CVSS (Common Vulnerability Scoring System), Türkçe'de "Ortak Zafiyet Puanlama Sistemi" olarak bilinen bir güvenlik ölçeğidir. CVSS, bir bilgisayar zafiyetinin ciddiyetini ve etkisini puanlamak için kullanılan bir metriktir. Bu puanlama sistemi, bir zafiyetin tehlike seviyesini belirlemek ve olası etkilerini değerlendirmek için kullanılan bir standartlaştırılmış bir yaklaşım sağlar.

CVSS, bir zafiyetin üç ana bileşenini değerlendirir:

* Temel Skor (Base Score): Zafiyetin, teknik açıdan ne kadar kolay sömürülebildiği, etkilenen sistemlerde ne kadar yetenek gerektirdiği ve zafiyetin etkilerinin ne kadar ciddi olduğu gibi faktörleri değerlendirir. Temel Skor, bir zafiyetin ciddiyetini ölçmek için kullanılır.
* Temporal Skor (Temporal Score): Zafiyetin yayılma hızı, saldırılarla ilgili bilgilerin yayılma durumu ve zafiyetin üzerindeki korumaların etkinliği gibi faktörleri değerlendirir. Temporal Skor, bir zafiyetin etkisini zamana göre değiştirir.
* Çevresel Skor (Environmental Score): Bir organizasyonun veya sistem sahibinin kendi çevresine özgü faktörleri dikkate alarak zafiyetin etkilerini değerlendirir. Bu faktörler arasında sistemlerin değeri, sistemlerin kritikliği, ağ yapılandırması ve güvenlik politikaları gibi etkenler yer alır.



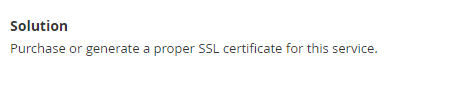
Şekil CVSS Zafiyet sınıflandırması

CVSS puanlama sistemi, 0 ile 10 arasında bir skor verir, 10 en yüksek riski, 0 ise en düşük riski temsil eder. Bu puanlama sistemi, zafiyetlerin aciliyet seviyelerini, önemlerini ve risk düzeylerini değerlendirmek için yaygın olarak kullanılır.

**ZAFİYET ÇÖZÜMÜ**

Tarama yapıldıktan ve zafiyetler raporlandıktan nessusun direktifleri ile, rahat bir şekilde zafiyetleri bertaraf edebiliriz. Zafiyete girdikten sonra açıklamalarının altında “Solution” da çözüm bizlere verilmiştir örnek olarak yaptığımız taramada “SSL Certificate Cannot Be Trusted” zafiyetini tespit ettik CVSS scoru 6.5 olan bu zafiyet medium sınıfında bir zafiyettir.

Çözümü için Nessusun direktiflerine baktığımızda “Bu servis için uygun bir SSL sertifikası al ya da yarat” cevabını alıyoruz servis sağlayıcı ile iletişime geçerek bu sorunu ortadan kaldırabiliriz



Şekil Zafiyet Çözümü

### TARAMA İŞLEMİNİ İZLEMEK İÇİN



## Kaynakça

<https://secromix.com/blog/nessus-guvenlik-acigi-tarama/>

<https://pwnlab.me/tr-nessus-nedir-kurulumu-ve-nessus-ile-zafiyet-taramasi/>

<https://secromix.com/blog/sizma-testi-bir-zorunluluk-mu/>

<https://www.beyaz.net/tr/guvenlik/makaleler/nesus_nedir_ve_ne_amacla_kullanilir.html>

M. A. Yalçınkaya and E. Küçüksille , "Web Uygulama Sızma Testlerinde Kapsam Genişletme İşlemi İçin Metodoloji Geliştirilmesi ve Uygulanması", *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 25, no. 1, pp. 16-27, Apr. 2021, doi:10.19113/sdufenbed.661867

T. Yiğit and M. Akyıldız , "Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi", *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 18, no. 1, pp. 14-21, Jun. 2014

Ö. F. Kaya and E. Öztürk , "VERİ VE AĞ GÜVENLİĞİ İÇİN UYGULAMA VE ANALİZ ÇALIŞMALARI", *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, vol. 16, no. 31, pp. 85-102, Jun. 2017