



İSTANBUL
GELİŞİM
ÜNİVERSİTESİ

**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

BEYAN

Bu ödevin/projenin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, ödevin/projenin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir ödev/proje olarak sunulmadığını beyan eder, aksi durumda karşılaşacağım cezai ve/veya hukuki durumu kabul eder; ayrıca üniversitenin ilgili yasa, yönerge ve metinlerini okuduğumu beyan ederim.

Tarih 02/06/2023

Adı Soyadı Mustafa Yurtolan



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 1 https://secromix.com/wp-content/uploads/2021/06/nessuslogo-02.png	7
Şekil 2 Tarayıcı da arama	8
Şekil 3 Doğru link	8
Şekil 4 Versiyon seçimi	8
Şekil 5 Lisans Sözleşmesi	8
Şekil 6 Install wizard	9
Şekil 7 Lisans sözleşmesi	9
Şekil 8 Klasör seçimi	9
Şekil 9 Kurulum başlatma onayı	10
Şekil 10 Kurulum bitiş ekranı	10
Şekil 11 Local host görünümü	10
Şekil 12 Welcome to Nessus	11
Şekil 13 Nessus varyasyonları	11
Şekil 14 Kayıt ekranı	12
Şekil 15 Kullanıcı adı ve parola	12
Şekil 16 Pluginler 5J8H-TLKY-4LPN-7ZDW-D55	12
Şekil 17 Nessusa giriş	13
Şekil 18 Scan arayüzü	13
Şekil 19 My Scans	13
Şekil 20 All Scans	13
Şekil 21 Trash	13
Şekil 22 Policies	14
Şekil 23 Plugin Rules	14
Şekil 24 Terrascan	14
Şekil 25 About	14
Şekil 26 Advanced	14
Şekil 27 Proxy Server	14
Şekil 28 SMTP Server	14
Şekil 29 Custom CA	15
Şekil 30 Custom CA	15
Şekil 31 Scanner Health	15
Şekil 32 Notifications	15
Şekil 33 My Account	15
Şekil 34 Politika özelleştirme	15
Şekil 35 Policies	16
Şekil 36 Advandec Scan arayüzü	17
Şekil 37 Gernal ön izleme	17
Şekil 38 Schedule	17
Şekil 39 Notifications	18
Şekil 40 Assesment	18
Şekil 41 Malware	19
Şekil 42 Hazır halde bir tarama	20
Şekil 43 Tarama Takibi	20
Şekil 44 Tarama Host Ekranı	21
Şekil 45 Vulnerabilities Sayfası	21
Şekil 46 Detaylı zafiyet listesi	21
Şekil 47 Detaylı zafiyet	22
Şekil 48 CVSS Zafiyet sınıflandırması	23
Şekil 49 Zafiyet Çözümü	23

İçindekiler

Beyan.....	ii
KABUL VE ONAY SAYFASI	3
ÖZET	1
Şekiller Listesi	2
ÖN SÖZ	4
GİRİŞ	5
1.1 Zaafiyet nedir.....	6
1.2 Pentesting Nedir.....	6
2.1 NESSUS NEDİR	6
2.2 Nessus ne için kullanılır.....	6
2.3 Nessus avantajları	7
2.4 Nessus kurulumu.....	7
3.1 Nessus arayüzü.....	13
3.2 Scan Arayüzü	13
Resources	13
Accounts.....	15
4.1 Zafiyet Taraması	15
4.2 Taramaya Başlanması.....	19
4.3 Zafiyet Çözümü	22
TARAMA İŞLEMİNİ İZLEMEK İÇİN	24
Kaynakça	25

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 indirmek 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 1 <https://secromix.com/wp-content/uploads/2021/06/nessuslogo-02.png>

Nessusun sunduğu güvenlik açıkları;

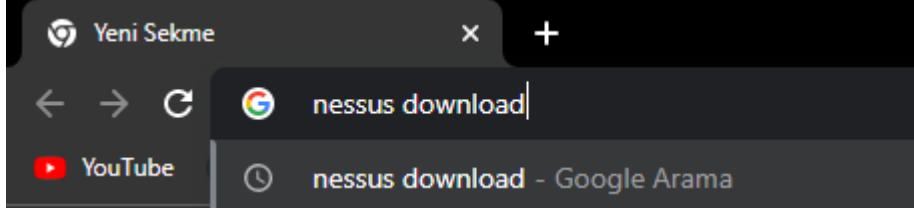
- Verilerin erişilip bunların kontrol edilmesine izin veren zafiyetler,
- Yanlış Kurma sorunlarının önceden bildirilmesi,
- Sistemdeki şifreler ile ilgili zafiyetlerin listelenmesi,
- DDOS saldırılarına açıklık veren TCP/IP sorunlarının görüntülenmesi,
- Hızlı bir şekilde varlık keşfi,
- Yama ve kurulum 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 olduğu 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.

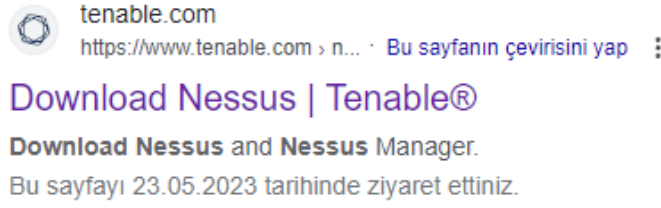
2.4 Nessus kurulumu

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



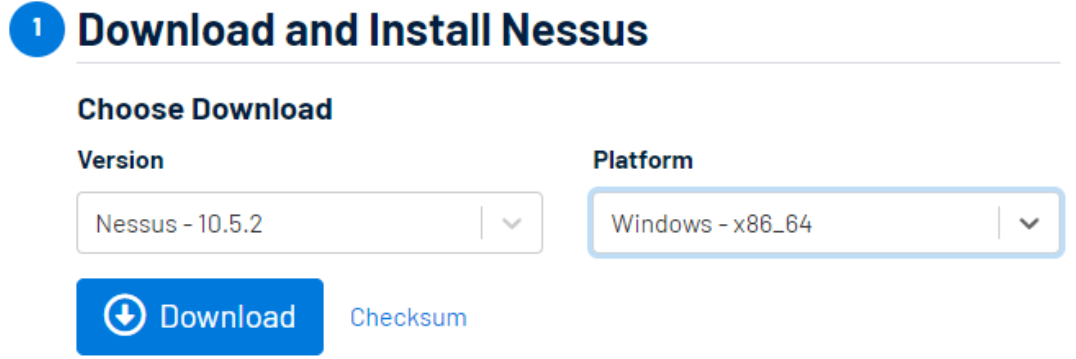
Şekil 2 Tarayıcı da aratma

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



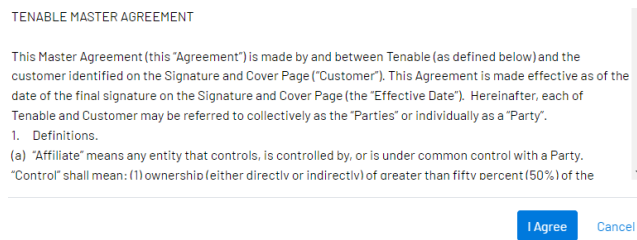
Şekil 3 Doğru link

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



Şekil 4 Versiyon seçimi

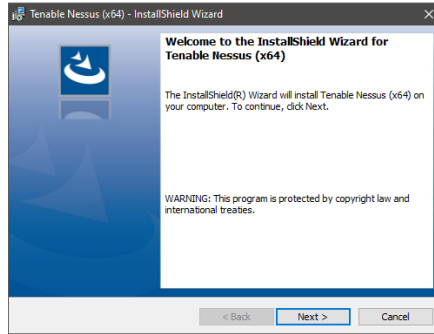
4. Download butonuna bastıktan sonra karşımıza çıkan lisans sözleşmesini onaylayalım.



Şekil 5 Lisans Sözleşmesi

I Agree dedikten sonra setup indirilmeye başlayacaktır.

Setup indirildikten sonra üzerine tıklayarak açalım



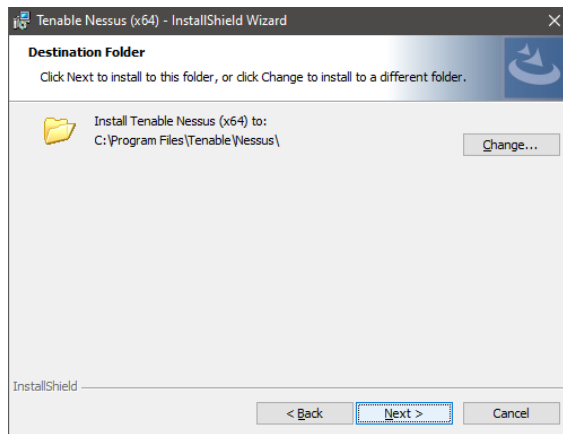
Şekil 6 Install wizard

- Next tuşuna basarak ilerleyelim karşımıza çıkan lisans sözleşmesini onaylayalım



Şekil 7 Lisans sözleşmesi

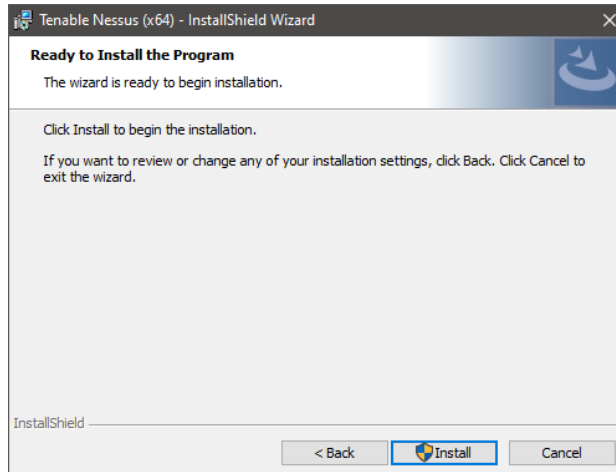
- Sözleşmeyi kabul ettikten sonra kurulumun yapılacağı klasörü seçelim



Şekil 8 Klasör seçimi

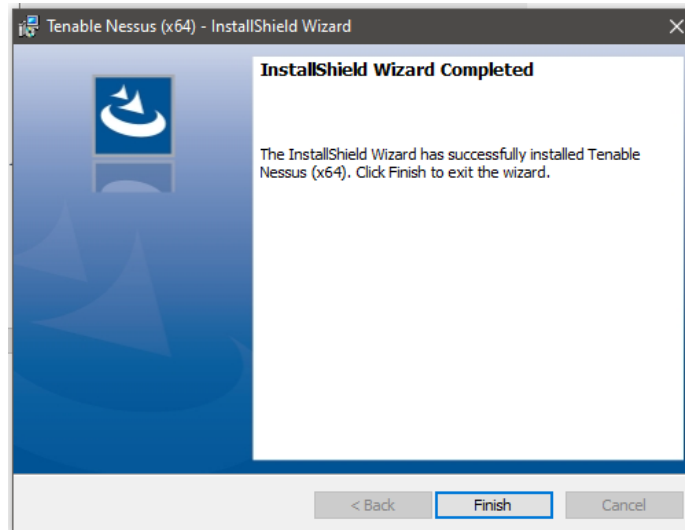
- Klasörü seçtikten sonra (Default olarak C klasörüne kuruyor) next diyerek kurulumu

başlayalım



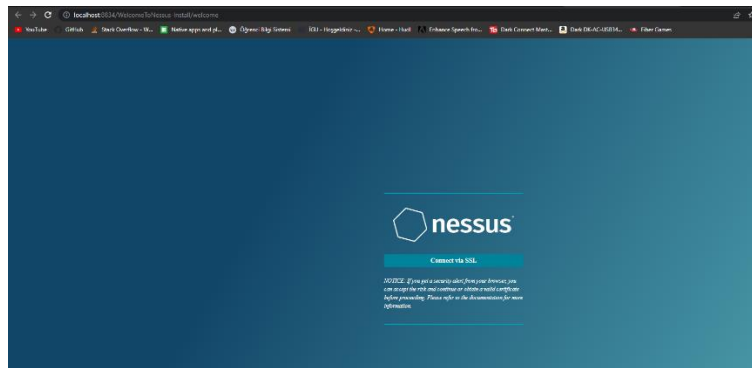
Şekil 9 Kurulum başlatma onayı

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



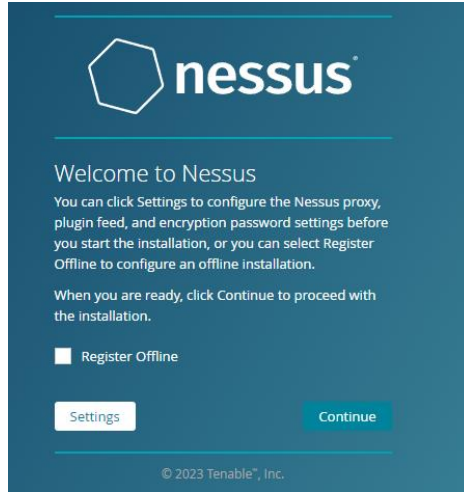
Şekil 10 Kurulum bitiş ekranı

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



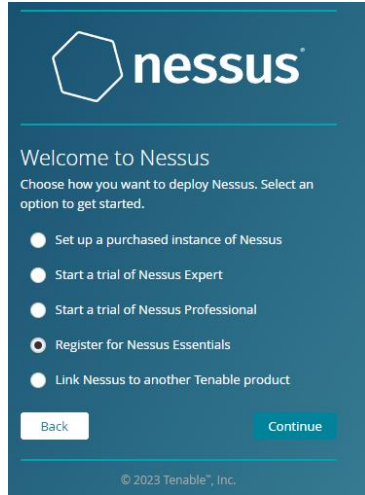
Şekil 11 Local host görünümü

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



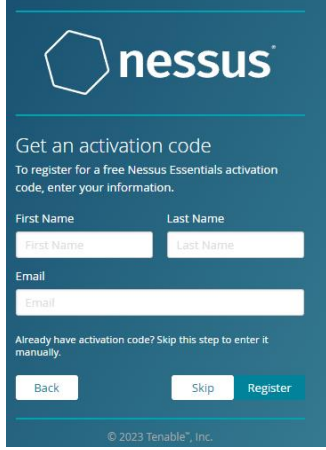
Şekil 12 Welcome to Nessus

11. 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.



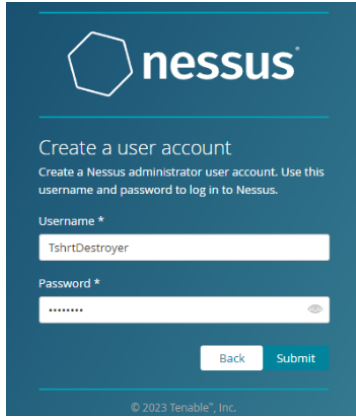
Şekil 13 Nessus varyasyonları

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

The image shows the Nessus registration page. At the top is the Nessus logo. Below it, the text "Get an activation code" is displayed, followed by "To register for a free Nessus Essentials activation code, enter your information." There are three input fields: "First Name", "Last Name", and "Email". Below these fields, there is a link that says "Already have activation code? Skip this step to enter it manually." At the bottom, there are three buttons: "Back", "Skip", and "Register". The footer contains the copyright notice "© 2023 Tenable, Inc."

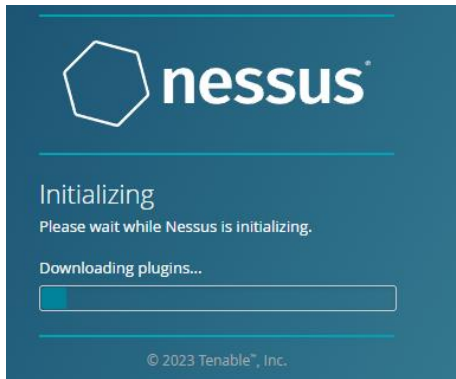
Şekil 14 Kayıt ekranı

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

The image shows the Nessus user account creation page. At the top is the Nessus logo. Below it, the text "Create a user account" is displayed, followed by "Create a Nessus administrator user account. Use this username and password to log in to Nessus." There are two input fields: "Username *" and "Password *". The "Username *" field contains the text "TshrtDestroyer". The "Password *" field contains a series of asterisks. Below these fields, there are two buttons: "Back" and "Submit". The footer contains the copyright notice "© 2023 Tenable, Inc."

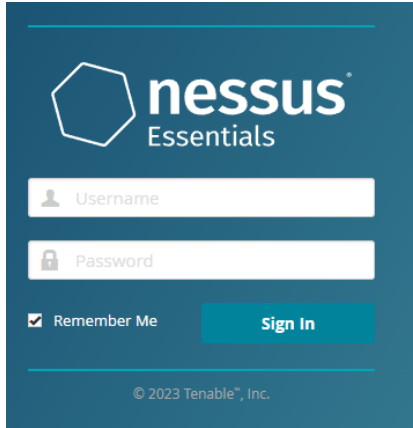
Şekil 15 Kullanıcı adı ve parola

14. Ardından gerekli pluginlerin indirilmesini bekleyin

The image shows the Nessus initialization screen. At the top is the Nessus logo. Below it, the text "Initializing" is displayed, followed by "Please wait while Nessus is initializing." There is a progress bar labeled "Downloading plugins..." which is partially filled. The footer contains the copyright notice "© 2023 Tenable, Inc."

Şekil 16 Pluginler

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



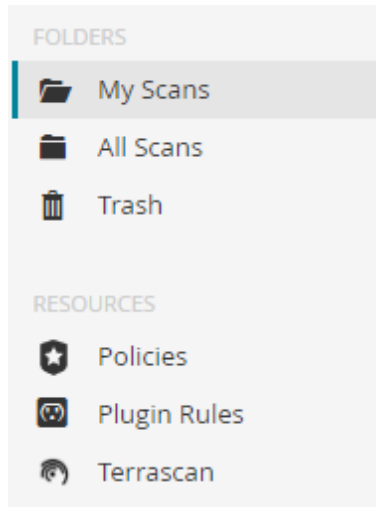
Şekil 17 Nessusa giriş

3.1 Nessus arayüzü

Nessus arayüzünü **Scan** ve **Settings** olarak 2 farklı şekilde anlatabiliriz. Scan arayüzünde taramalar hakkında bilgilere ulaşarak bunları görüntüleyebiliriz. Settings kısmında aracın detaylı ayarlarını manuel bir şekilde değiştirebiliriz.

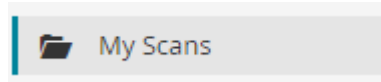
3.2 Scan Arayüzü

Scan arayüzünde **folder** altında bulunan özellikler;



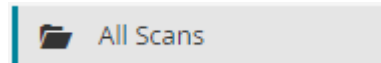
Şekil 18 Scan arayüzü

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



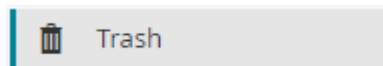
Şekil 19 My Scans

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



Şekil 20 All Scans

3. Trash: Silinen taramaların depolandığı klasördür.



Şekil 21 Trash

Resources altında bulunan özellikler ise;

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



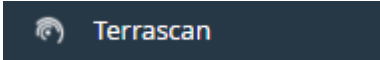
Şekil 22 Policies

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



Şekil 23 Plugin Rules

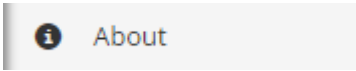
3. Terrascan: Statik bir kod altyapısıdır, farklı şekillerde kurulup kullanılabilir.



Şekil 24 Terrascan

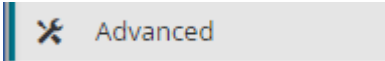
Settings kısmına geldiğimizde ise bizi settings ve accounts adlı iki alan karşılıyor bunlardan settings altında;

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



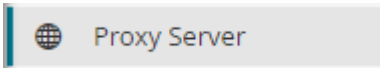
Şekil 25 About

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



Şekil 26 Advanced

3. Proxy Server: Https isteklerini iletmek için kullanılır bu bağlantının bilgileri buradan görüntülenebilir.



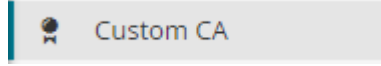
Şekil 27 Proxy Server

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



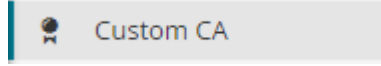
Şekil 28 SMTP Server

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



Şekil 29 Custom CA

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



Şekil 30 Custom CA

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



Şekil 31 Scanner Health

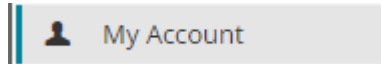
8. Notifications: Nessusun ilk indirildiği andan itibaren hangi tarihte hangi işlemlerin yapıldığının bilgisi listelenir



Şekil 32 Notifications

Accounts altında tek bir özellik bulunur;

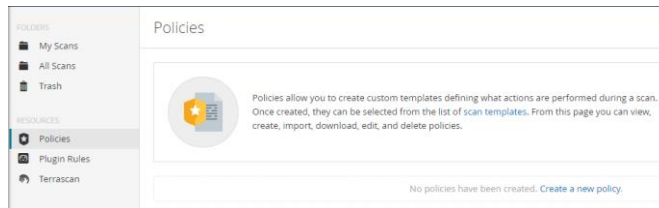
1. My Account: Hesap hakkında kullanıcı adı,email,parola gibi bilgilerin bulunduğu alandır apı keyse de buradan ulaşılabilir ve nessus apisi ile doğrulama yapılabilir



Şekil 33 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.



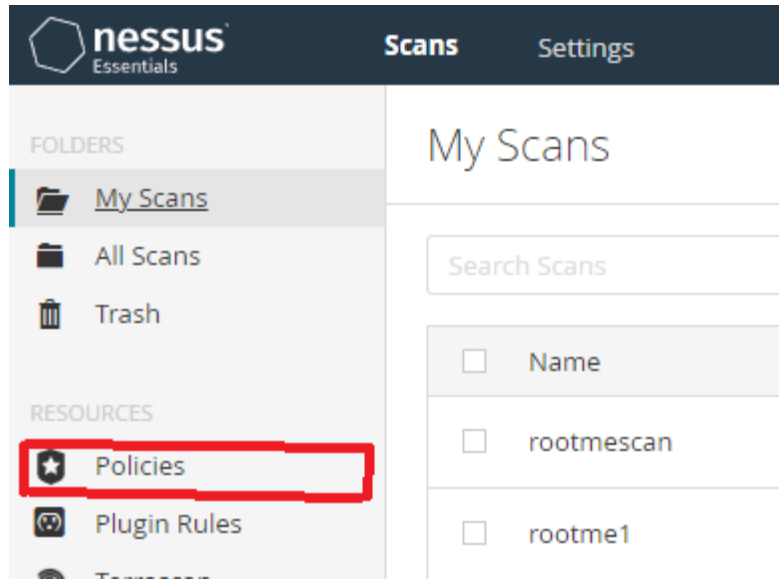
Şekil 34 Politika özelleştirme

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.

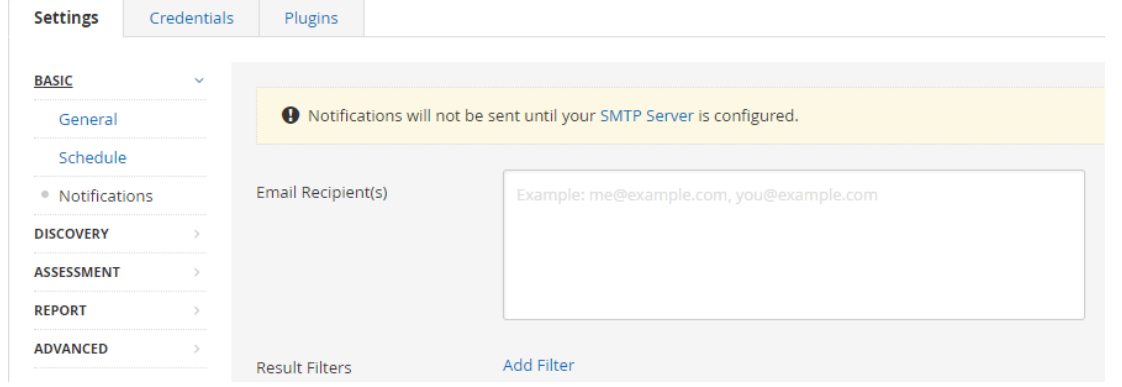
Nessus ile zafiyet taraması gerçekleştirmek için sırası ile şu adımlar gerçekleştirilebilir.

1. Scans sayfasında Resources altında bulunan "Policies" sekmesine gelinir



Şekil 35 Policies

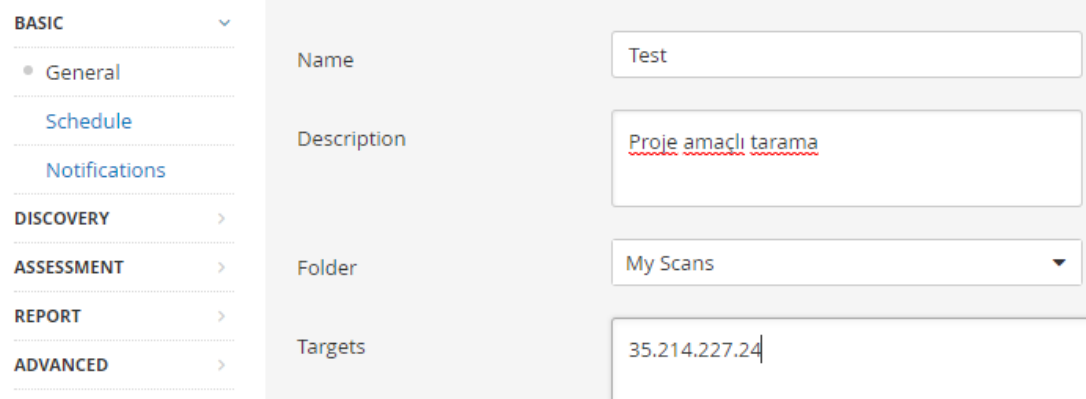
2. Policies sayfasında daha önce oluşturulan tarama taslaklarını görüntüleyebilir. Ve bunların arasına yeni taslaklar ekleyebiliriz. Scan templates'e tıkladıktan sonra karşımıza çıkan sayfadan Scanner altından hazır tarama ve zafiyet bulma işlemlerinden birini seçebilir veya ta spesifik bir işlem için "User Defined" sayfasından yeni bir taslak oluşturabilir yada var olan bir taslağı kullanabiliriz. Vulnerabilities altında bulunan "Advanced Scan" e tıklayarak işleme devam edebiliriz
3. Karşımıza gelen sayfada bizi 3 adet kısım karşılıyor Settings, Credentials ve Plugins



Şekil 36 Advandec Scan arayüzü

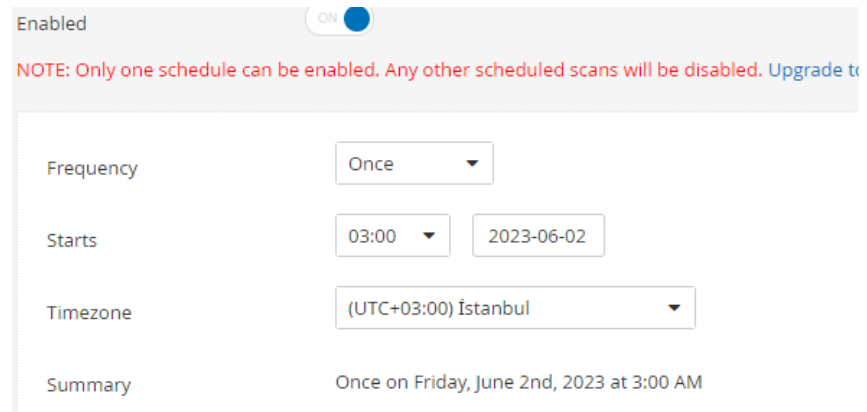
Sırası ile açıklamak gerekirse:

- **Settings:** Tüm ayarların bulunduğu kısımdır kendi altında Basic, Discovery, 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



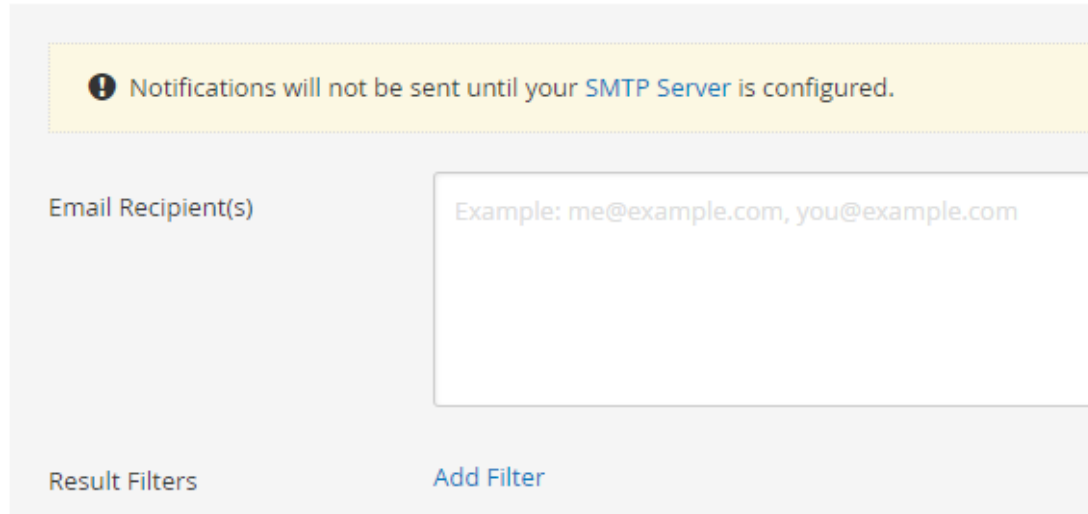
Şekil 37 General ön izleme

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



Şekil 38 Schedule

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

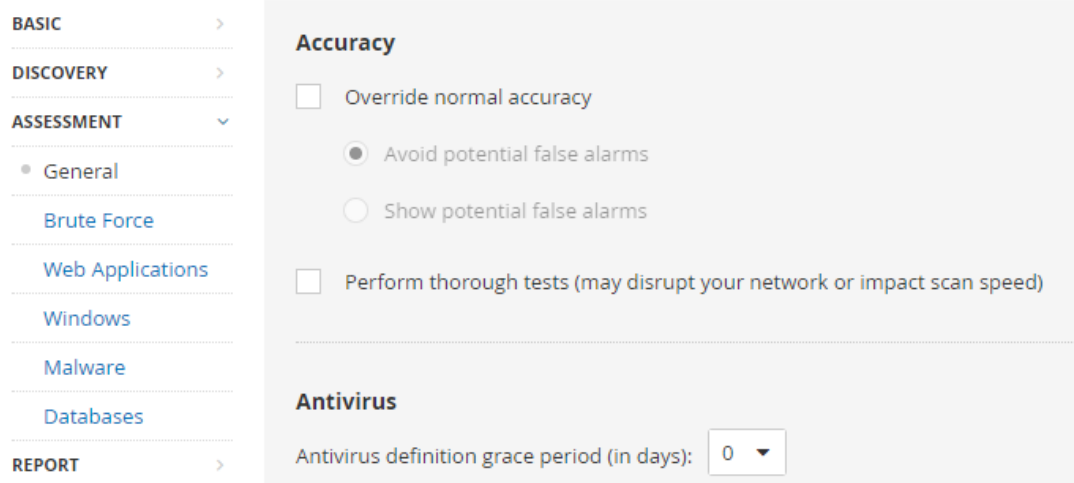


Şekil 39 Notifications

Discovery 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.

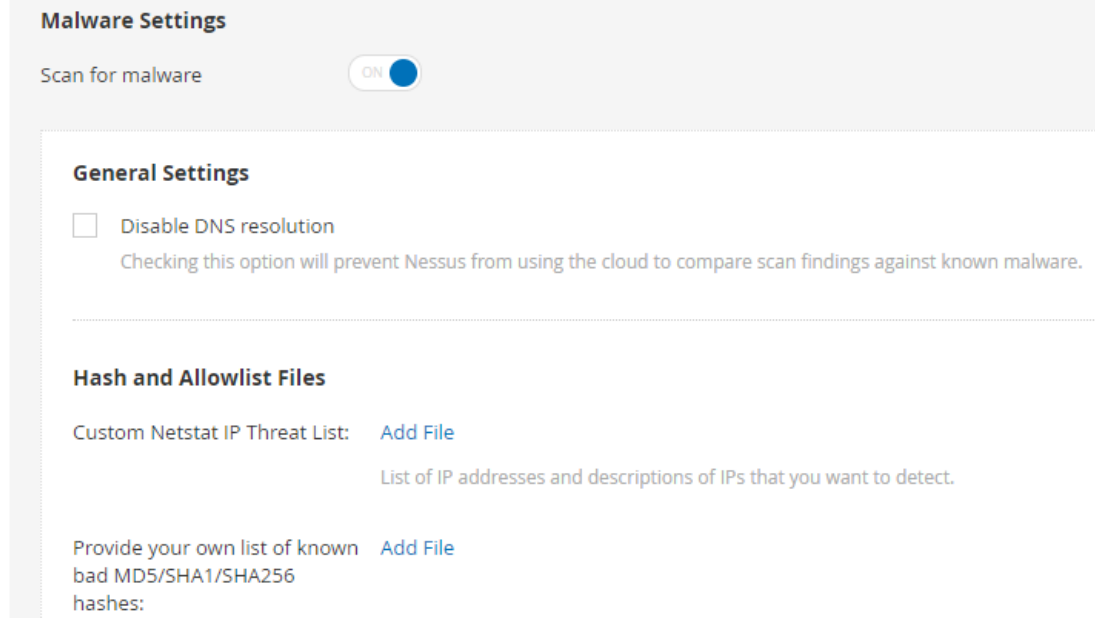
Assesment kısmı Discoveryin aksine saldırı odaklı ayarlamaları yapabiliriz.



Şekil 40 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 41 Malware

Report Sekmesi ile tarama sonucunda kimlere nelerin raporunun gideceğini özelleştirebiliriz.

Advanced sekmesi Taramanın performansı ile, 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 adresi Tanımlanır ve sol altta bulunan Launch butonu ile tarama gerçekleştirilmeye başlanır.

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

ProjeDeneme1

Description

Proje için tarama

Folder

My Scans

Targets

35.214.227.24

Upload Targets

Add File

Save

Cancel

Launch

Şekil 42 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

My Scans				Import	New Folder	New Scan
Search Scans				11 Scans		
<input type="checkbox"/>	Name	Schedule	Last Scanned			
<input type="checkbox"/>	ProjeDeneme1	On Demand	Today at 3:57 AM	▶	✕	
<input type="checkbox"/>	rootmescan	On Demand	May 27 at 6:17 PM	▶	✕	
<input type="checkbox"/>	rootme1	On Demand	May 27 at 6:17 PM	▶	✕	
<input type="checkbox"/>	sudo6	On Demand	May 27 at 6:12 PM	▶	✕	
<input type="checkbox"/>	sudo5	On Demand	May 27 at 6:09 PM	▶	✕	
<input type="checkbox"/>	sudo4	On Demand	May 27 at 5:55 PM	▶	✕	
<input type="checkbox"/>	AgentSudo3	On Demand	May 27 at 5:54 PM	▶	✕	
<input type="checkbox"/>	AgentSudo2	On Demand	May 27 at 5:44 PM	▶	✕	
<input type="checkbox"/>	AgentSudo	On Demand	May 27 at 5:41 PM	▶	✕	
<input type="checkbox"/>	ideneme2	On Demand	May 27 at 4:01 PM	▶	✕	
<input type="checkbox"/>	Deneme	On Demand	May 27 at 3:42 PM	▶	✕	

Şekil 43 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

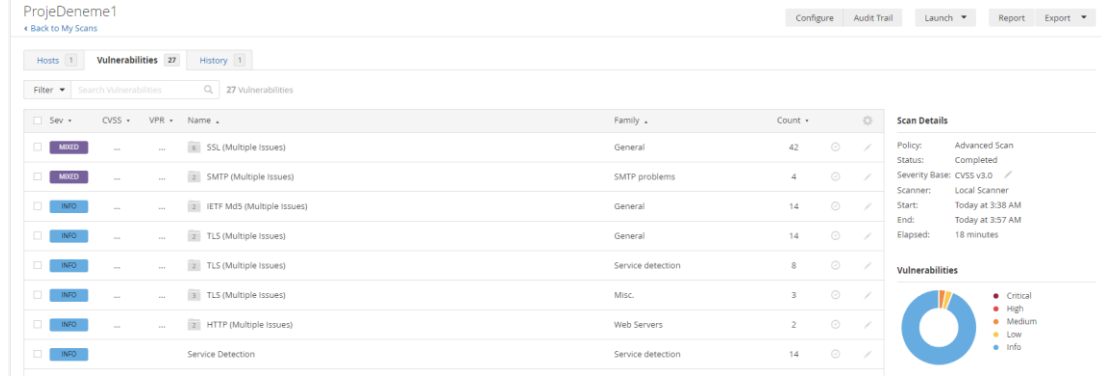
süreç saatleri bulabilir.

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.



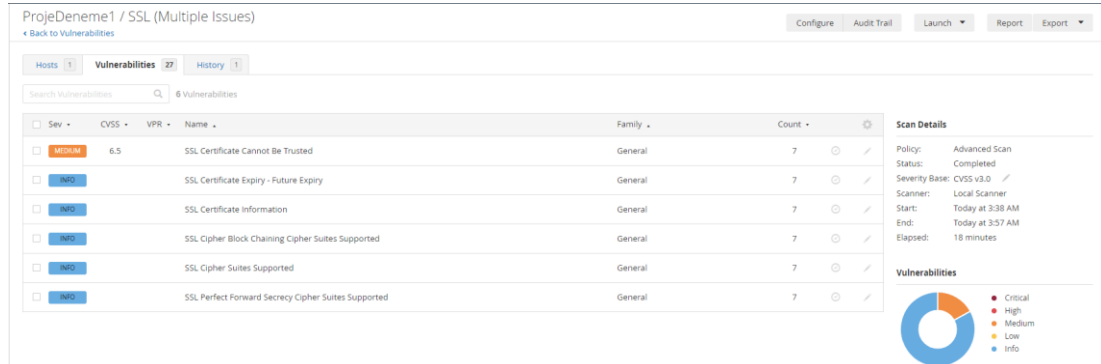
Şekil 44 Tarama Host Ekranı

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 sayıldığına bilgilerine ulaşabiliriz.



Şekil 45 Vulnerabilities Sayfası

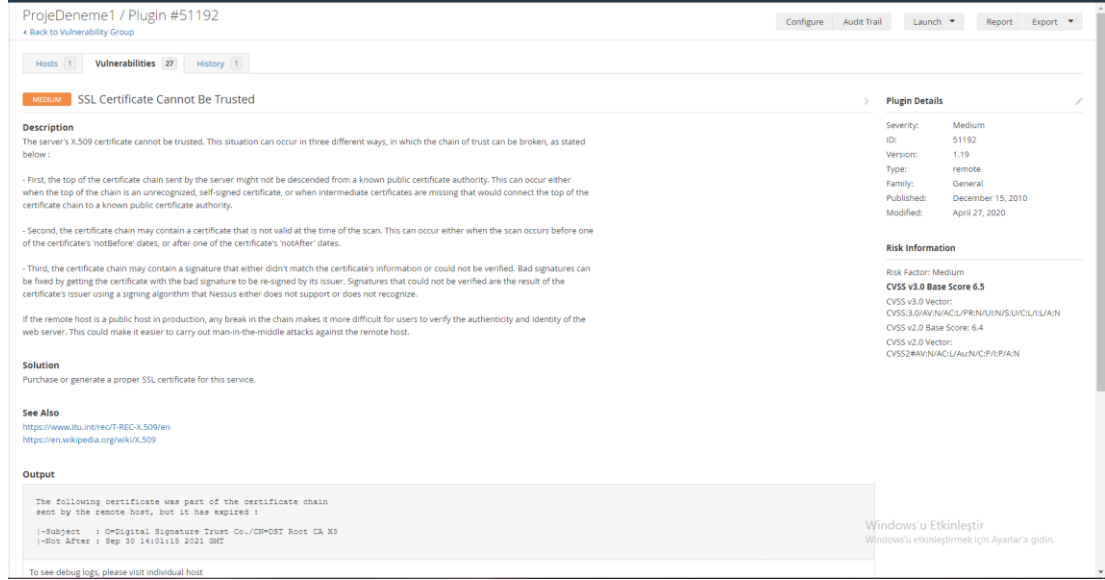
Listelenen zafiyetlerden birine girdiğimiz de detaylı bir şekilde o zafiyet hakkında bilgiler bizi karşılıyor yine adı, CVSS değeri, familyası gibi genel bilgilerin dışında



Şekil 46 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 47 Detaylı zafiyet

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

4.3 Zafiyet Çözümü

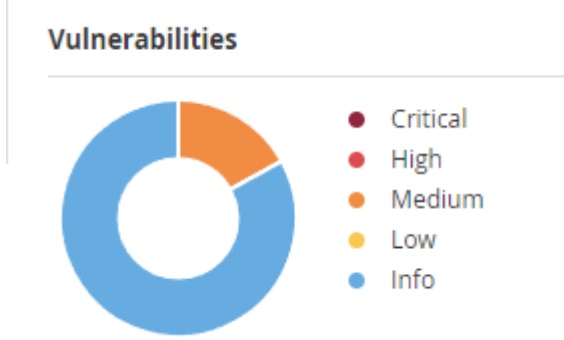
CVSS NEDİR

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 48 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 skoru 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 kaldıracaktır.

Solution

Purchase or generate a proper SSL certificate for this service.

Şekil 49 Zafiyet Çözümü

TARAMA İŞLEMİNİ İZLEMEK İÇİN



Beni tara!

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/nessus_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