

Nessus Kullanım Kitapçığı

[Nessus 4.2 El Kitabı]

Gökay Bekşen
gokay@lifeoverip.net

[Bu yazıda de fakto internet güvenlik tarayıcısı Nessus'un 4.2 sürümü detaylı anlatılmıştır.]

İçerik Tablosu

1. Nessus 4.2.....	4
2. Pluginler.....	4
3. Bağlantı Kurma.....	5
a. Nessus Client Uygulaması.....	6
b. Nessus Client Web Arayüzü	7
4. Tarama Yapmak	8
5. Raporlama	9
a. Rapor Filtreleri.....	9
b. Rapor Formatları	10
6. Tarama Profilleri (Policy)	10
a. General	11
i. Basic.....	11
ii. Scan.....	11
iii. Network Congestion	12
iv. Port Scanners	12
v. Port Scan Options	13
vi. Performance.....	13
b. Credentials.....	13
i. Windows Credentials.....	13
ii. SSH Credentials	14
iii. Oracle Settings	14
iv. Kerberos Configuration.....	14
v. Cleartext Protocol Settings	14
c. Plugins	15
d. Preferences.....	15
i. Database Compliance Checks	15
ii. Do not Scan Fragile Devices	15
iii. Global Variable Settings.....	15
iv. HTTP Login Page	16
v. ICCP/COTP TSAP Addressing	17
vi. Login Configurations.....	17
vii. Modbus/TCP Coil Access.....	17
viii. Nessus SYN Scanner ve Nessus TCP Scanner.....	17

ix.	News Server (NNTP) Information Disclosure	17
x.	PCI DSS Compliance	18
xi.	Ping the Remote Host	18
xii.	Port Scanner Settings.....	18
xiii.	SMB Registry: Start the Registry Service during the scan	18
xiv.	SMB Scope.....	19
xv.	SMB use domain SID to enumerate users.....	19
xvi.	SMB use host SID to enumerate local users.....	19
xvii.	SMTP Settings.....	19
xviii.	SNMP Settings	19
xix.	Service Detection.....	20
xx.	Unix Compliance Check.....	20
xxi.	Web Application Test Settings	20
xxii.	Web Mirroring.....	21
xxiii.	Windows Compliance Check	21
xxiv.	Windows File Contents Compliance Checks	21
7.	Kullanıcılar	21

1. Nessus 4.2

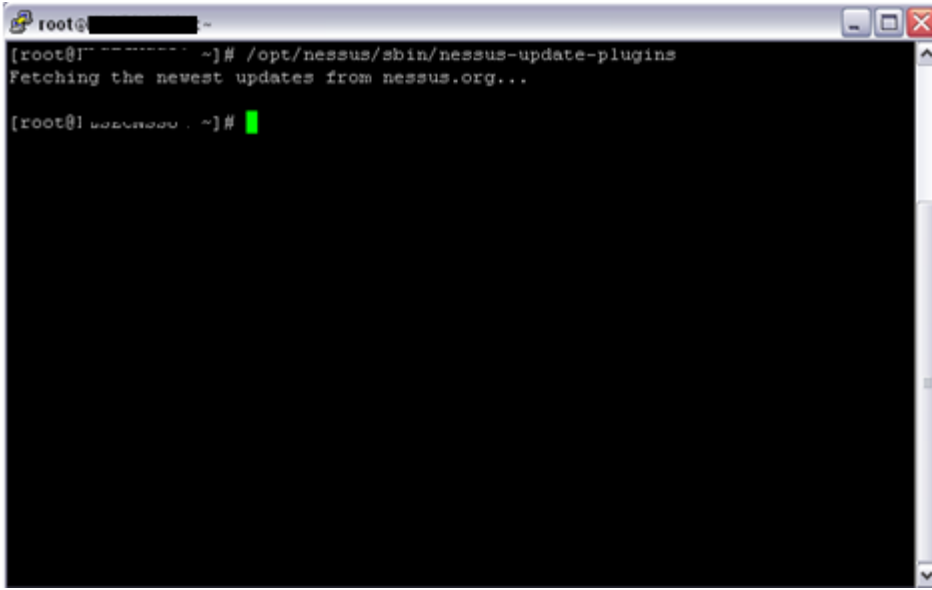
Nessus, bir güvenlik aracı olup fiziksel taramalar ve zafiyet analizleri için kullanılan bir uygulamadır. Oluşturulacak tarama profilleri vasıtasıyla, bütün bir network veya belirli hostlar taranabilir, güvenlik açıklıkları keşfedilebilir.

2. Pluginler

Nessus 4.2 Professional Feed versiyonuna ait olan pluginler, bir taramanın davranışlarını ve kapsamalarını belirlemek için kullanılır. İlerleyen bölümlerde anlatılacak olan tarama profillerinde, değişik tarama türlerine göre farklı pluginler kullanılacağı ve çeşitli uyarılar hakkında bilgi verilecektir.

Tarama sonuçlarının güncel olması açısından pluginler güncelleştirilmelidir. Varsayılan olarak Nessus tarayıcı pluginlerini 24 saatte bir güncelleştirmeye çalışır. El ile güncelleştirmeye ait komut bilgileri ve ekran görüntüleri aşağıdaki gibidir :

- Güncelleştirme komutu : `/opt/nessus/sbin/nessus-update-plugins`
- Güncelleştirme ekran görüntüsü :



```
root@ [redacted] ~# /opt/nessus/sbin/nessus-update-plugins
Fetching the newest updates from nessus.org...

[root@ [redacted] ~]#
```

Pluginlerin otomatik olarak güncelleştirilmesine ait komut bilgileri ve ekran görüntüleri aşağıdaki gibidir :

- `cd /opt/nessus/etc/nessus` dizinine ulaşılır.

```
root@ [redacted] /opt/nessus/etc/nessus
[root@ [redacted] ]# cd /opt/nessus/etc/nessus/
[root@ [redacted] nessus]# ls
nessusd.conf  nessusd.rules  nessus-fetch.rc  nessus-fetch.rc.dist
[root@ [redacted] nessus]# vi nessusd.conf
```

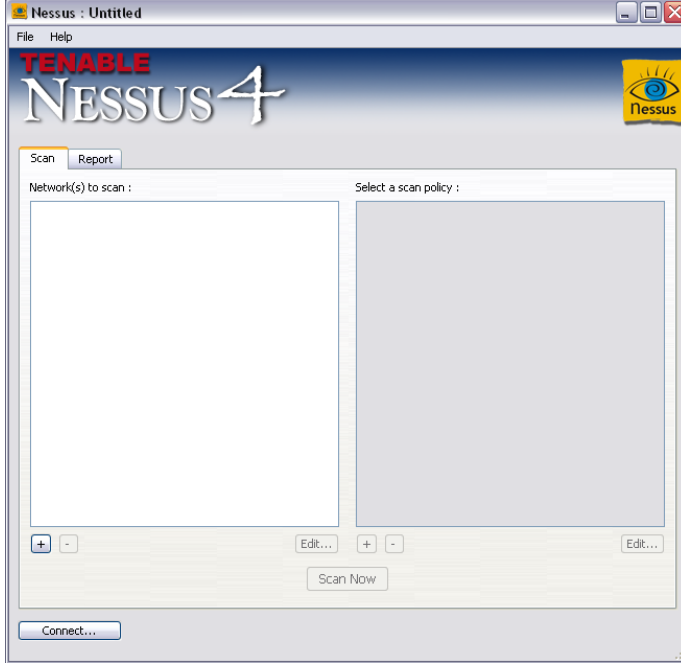
- Vi nessusd.conf komutu ile otomatik güncelleştirme bilgisinin bulunduğu dosya açılır. İki güncelleştirme arasındaki zaman ok ile belirtilmiştir (varsayılan olarak 24 saattir).

```
root@ [redacted] /opt/nessus/etc/nessus
# Configuration file of the Nessus Security Scanner
#
# Any line starting with a '#' is a comment and will be
# ignored by the Nessus Scanner
#
# Automatic plugins
# If enabled and Nessus is registered, then
# fetch the newest plugins from plugins.nessus.org automatically. Disable
# if the scanner is on a restricted network not able to reach the Internet.
auto_update = yes
# Number of hours to wait between two updates
auto_update_delay = 24
# Should we purge the plugin database at each update ? (slower)
purge_plugin_db = no
# Maximum number of simultaneous hosts tested :
max_hosts = 60
```

3. Bağlantı Kurma

Nessus, bir server bir de client olmak üzere iki parçalı bir yapıya sahiptir. Tarama ve zafiyet analizi isteklerini oluşturan client servera iki şekilde bağlanır:

a. Nessus Client Uygulaması



Uygulama Nessus Servera bağlanmak için kullanılır. Bu uygulama vasıtasıyla taramalar gerçekleştirilir, tarama sonuçları gösterilir. İlgili rapor uygulama sayesinde indirilebilir. Client programı vasıtasıyla Nessus servera bağlanmak için aşağıdaki adımlar izlenmelidir :

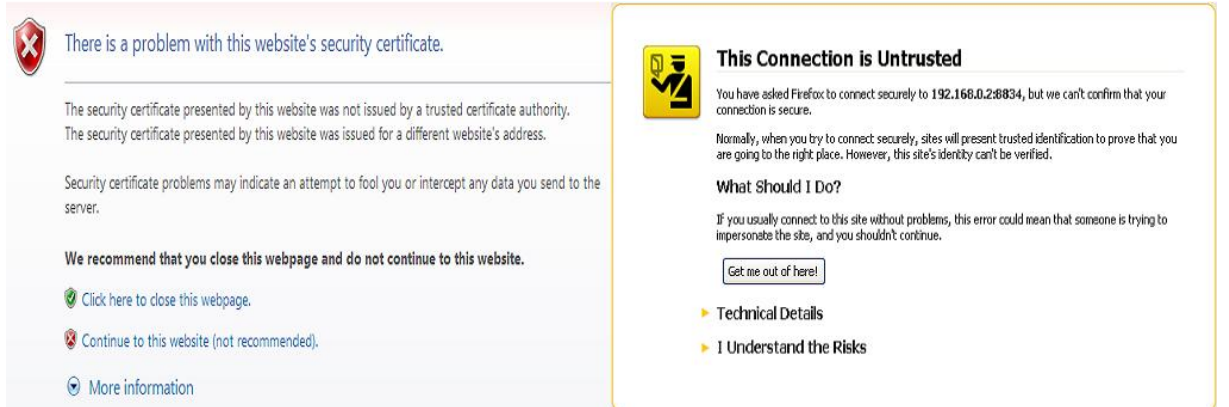
1. Sol altta bulunan connect tuşuna basın.
2. Karşınıza çıkan Connection Manager bannerlı pop-up ekranının sol alt kısmında bulunan artı (+) tuşuna basın.
3. Edit connection bannerlı yeni ekranda aşağıda belirtilen boş alanların doldurulması gerekmektedir:
 - a. Connection name, oluşturacağınız yeni bağlantının ismini belirtir.
 - b. Host name, Nessus Serverın üzerinde koştugu servera ait IP adresi.
 - c. Port, Nessus Servera erişilecek olan port numarası. Varsayılan olarak 1241 nolu porttur.
 - d. Login, Nessus Servera bağlanmak için gerekli olan kullanıcı ismidir.
 - e. Password, Nessus Servera bağlanmak için gerekli olan kullanıcı ismine ait şifredir.
4. Save tuşuna basarak yeni bağlantı kaydedilir.
5. Ekranda yeniden belirecek olan Connection Manager ekranında bağlanılmak istenilen Nessus Server seçilir ve sağ altta bulunan connect tuşuna basılır.
6. İlk defa bağlanması durumunda, Nessus Servera ait olan Hash numarasının kabulünü gerektiren ekran belirecektir. Hashi kabul ettikten sonra serverla bağlantı kurulur.
7. Bağlantının kapatılması için sol alttaki disconnect tuşuna basılması gerekmektedir.

b. Nessus Client Web Arayüzü



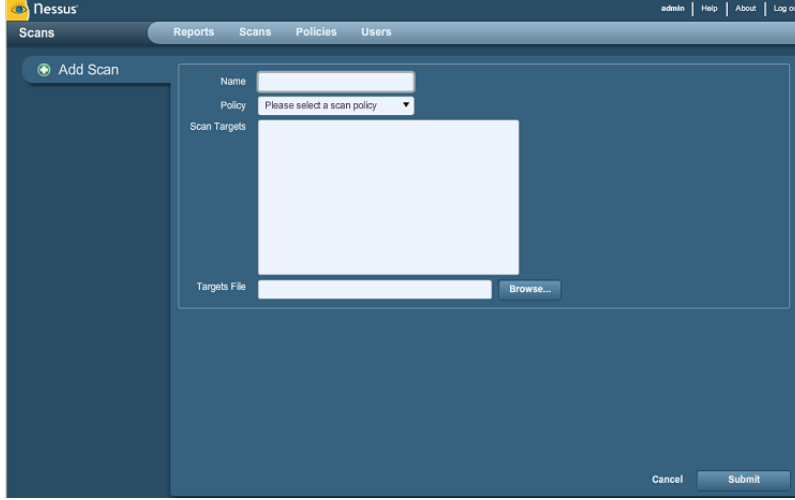
Web arayüzü Nessus Servera bağlanmak için kullanılır. Bu arayüz vasıtasıyla taramalar gerçekleştirilir, tarama sonuçları gösterilir. İlgili rapor arayüz sayesinde indirilebilir. Nessus Client Web Arayüzü vasıtasıyla Nessus servera bağlanmak için aşağıdaki adımlar izlenmelidir :

1. Internet Explorer ya da Mozilla Firefox browserında adres çubuğuna https://nessus_server_ip:8834/ adresi girilir.
2. Username ve password bilgileri girilir.
3. Log In tuşuna basılır.
4. Eğer ilk kez Web Arayüzüne giriş yapılıyorsa aşağıdakiler gibi uyarı alınması normaldir. Bu durumlar Nessus Servera ait olan sertifikanın, sizin bilgisayarınız tarafından kabul edilmesi ile bir daha gözükmeyecektir:



4. Tarama Yapmak

Tarama profili yaratıldıktan sonra, “Scans” seçeneğine basarak tarama bölümüne geçilir. Yukarı sağ kısımda “+Add” tuşuna basılır ve “Add Scan” isimli ekran gözükür. Bu ekranda yapılmak istenen tarama hakkında bilgiler girilir.



Bu ekrandaki bileşenler aşağıdaki gibidir :

- Name, oluşturulan taramanın ismini belirtir.
- Policy, yapılacak taramanın hangi profil üzerinden gerçekleşeceğini belirtir.
- Scan Targets, taranacak hostları belirtir. Çözülebilir host ismi veya tek bir ip girilebileceği gibi birden fazla hostlar için aralıklar kullanılabilir. Mesela, 192.168.0.1-192.168.0.255 veya 192.168.0.1/24
- Targets File, taranacak hostların bir text dosyası içerisine yazılıp, Web Arayüzüne upload edildikten sonra kullanılacağını belirtir.

Tarama bilgileri girildikten sonra “Submit” tuşuna basılır ve tarama başlar. Tek bir tarama veya birden fazla taramanın anlık görüntüsü aşağıdaki gibidir :



Name	Owner	Status	Start Time
HR Subnet	admin	41 IPs / 509 IPs	Nov 22, 2009 21:54
Linux Boxes	admin	0 IPs / 1 IPs	Nov 22, 2009 21:55

Tarama başladıktan sonra, tarama içeriği ile bilgi almak için “Browse” tuşuna basılabilir. Taramanın duraklatılması için “Pause”, devam etmesi için “Resume” veya durdurulması için “Stop” tuşlarına basılabilir.

Tarama bittikten sonra, taramayı ekrandan kaldırılabilir. Oluşacak çıktı “Report” bölümünün altında bulunacaktır.

5. Raporlama

“Reports” tuşuna basılarak raporlar bölümüne geçilir. Bu bölümün ekran görüntüsü aşağıdaki gibidir :



Name	Status	Last Updated
Dev Subnet	Completed	Nov 3, 2009 24:35
HR Subnet	Running	Nov 3, 2009 24:38
Local Desktop	Completed	Nov 3, 2009 24:40

“Reports” bölümünün bileşenleri aşağıdaki gibidir :

- Browse, oluşan raporların içeriklerini belirtir. Rapor içerisinde, host, port veya özellikle belirtilmiş olan zafiyetlere göre sonuçlar gözlemlenebilir.
- Compare, oluşturulan iki raporun karşılaştırılmasını belirtir.
- Upload, daha önceden oluşturulan bir raporun yeniden incelenmesi veya raporun versiyonunu değiştirmek için kullanılmasını belirtir.
- Download, biten bir tarama sonucu oluşan raporu bilgisayarımıza indirebileceğimizi belirtir.
- Delete, oluşturulan raporun silineceğini belirtir.

a. Rapor Filtreleri

Oluşturulan rapor içerisinde istenilen detaylara erişmek için filtreleme kullanılır. Sol taraftaki menüden “Show Filters” seçeneği ile aşağıda bileşenleri belirtilen filtreler kullanılabilir :

- Plugin ID, istenilen pluginlerin ID numaralarına göre filtreleme yapılacağını belirtir.
- Plugin Name, istenilen pluginlerin isimlerine göre filtreleme yapılacağını belirtir.
- Vulnerability Text, istenilen bir zafiyete göre filtreleme yapılacağını belirtir.
- Host, istenilen hostlara göre filtreleme yapılacağını belirtir.
- Ports, istenilen portlara göre filtreleme yapılacağını belirtir.
- Protocol, istenilen protokollere göre filtreleme yapılacağını belirtir.
- Severity, istenilen risk seviyesine göre filtreleme yapılacağını belirtir.

b. Rapor Formatları

- .nessus, Nessus 4.2 versiyonun önemli bir standardı olan, XML tabanlı rapor türüdür.
- .nessus (v1), Nessus 3.2 ile Nessus 4.0.2 versiyonları arasında kullanılan, XML tabanlı rapor türüdür. Nessus 4.2 ile uyumludur.
- HTML export, herhangi bir browserda görüntülenebilen standart HTML tabanlı rapordur.
- NBE export, csv uzantılı rapor tipidir.

6. Tarama Profilleri (Policy)

Nessus Server ile tarama yapabilmek için öncelikle tarama profilleri oluşturulmalıdır. Tarama profilini oluşturmadan önce, profilin kapsamı ve istenilen sonuçlar belirlenmeli ve profil bunlara göre oluşturulmalıdır. Herhangi bir profilin kapsamına ait olmayacak şekilde yapılan taramalar zaman kayıplarına, performansın düşmesine ve istenilen sonuçların elde edilememesine sebep olabilir.

Tarama profilleri oluştururken aşağıda açıklaması verilen gerekli bileşenler tercih edilmelidir. Farklı tiplerdeki hostlar, farklı kapsamlarda oluşturulan ve farklı bileşenleri olan profillerle taranmalıdır. Tarama profili oluşturmak için yukarıda bulunan bölümlerden “Policy” seçilmelidir.



Name	Visibility	Owner
LAN Scan	Private	admin

Daha sonra “add” tuşuna basıp yeni profil eklenebilir. Ekleme istediğiniz profile ait bileşenlerin bilgileri aşağıdaki gibidir :

a. General

i. Basic

- Name, profilin ismidir.
- Visibility, profil “shared” yani herkes tarafından kullanılabilir veya “private” sadece belirli bir kullanıcıya aittir.
- Description, profilin açıklamasıdır.

ii. Scan

- Save Knowledge Base, Nessus Server tarama bilgisini ileride kullanılabilmesi için Nessus Server knowledge base altına saklar.
- Safe Checks, hedef host üzerinde negatif etki yaratabilecek pluginleri seçilemez kılar.
- Silent Dependencies, eğer bu seçenek tercih edilirse, bir sisteme bağlı olan bitişik sistemler gösterilmez.
- Log Scan Details to Server, taramaya ait olan ek bilgileri Nessus Server loguna yazar. Bu şekilde hangi pluginlerin kullanılıp, hangi hostların tarandığı öğrenilebilir.
- Stop Host Scan on Disconnect, bu seçenek tercih edildiğinde Nessus Server bir hostun taranması esnasında hosta erişilememe durumunda, kullanıcının bilgisayarı kapatması veya yapılan taramayı bir güvenlik aygıtının DoS saldırısı olarak görüp trafiği engellemesi sonucunda, taramayı durdurur. Bu tercih seçilmezse, kapalı hostlar taranmaya devam edecek, gereksiz trafik oluşacak ve taramanın bitişi gecikecektir.

- Avoid Sequential Scans, Nessus Server taranacak olan ip adreslerini varsayılan olarak veriliş sırasına göre tarar. Bu seçenek seçildiğinde Nessus Server rastgele bir sırayla taramaya başlar. Bu şekilde, büyük kapsamlı taramalar yaparken network trafiğinin dağıtılmasına yardımcı olur
- Consider Unscanned Port as Closed, bu tercih seçilerek eğer bir port kapsam içerisinde belirtilmemişse, taranmamışsa o port kapalı olarak bildirilecektir.
- Designate Hosts by their DNS Name, çıktı olarak rapor alınırken, hostları ip adresleri yerine DNS isimleri bildirir.

iii. Network Congestion

- Reduce Parallel Connections on Congestion, bu seçenek vasıtasıyla Nessus, çok fazla paket gönderip network hattının kapasitesine yaklaşması durumunda bunu algılayabilir. Eğer algılanırsa, Nessus taramayı düzenler ve tıkanıklığı hafifletir. Tıkanıklık giderildikten sonra, Nessus otomatik olarak network hattındaki boş kısmı kullanmaya çalışacaktır.
- Use Kernel Congestion Detection (Linux Only), bu seçenek vasıtasıyla Nessus, üzerinde çalıştığı serverın işlemcisini ve diğer iç bileşenleri tıkanmaya karşın inceleyecek ve gerekli durumda ayarlayacaktır. Nessus kullanabildiği kadar çok kaynak tüketecektir. Bu özellik sadece eğer Nessus linux server üzerinde çalışırsa kullanılabilir.

iv. Port Scanners

- TCP Scan, Nessusa gömülü olarak gelen TCP tarayıcısı, hedefteki açık TCP portlarını tayin etmek için kullanılır. Bu tarayıcı optimize edilmiş ve kendisini geliştirebilen özelliklere sahiptir. **Uyarı: Bazı platformlarda (Windows, Mac OS X) TCP tarayıcısını kullanım halindeyken işletim sistemi ciddi performans sorunları oluşturursa, Nessus SYN tarayıcısını kullanacaktır.**
- UDP Scan, Nessusa gömülü olarak gelen UDP tarayıcısı, hedefteki açık UDP portlarını tayin etmek için kullanılır. **Uyarı: UDP, “stateless” yani iletişimi üçlü el sıkışma(three way handshake) ile gerçekleştirmeyen bir protokoldür. UDP tabanlı iletişim her zaman güvenilir değildir ve UDP servislerinin ve eleme aygıtlarının doğasından ötürü, her zaman uzaktan farkedilebilir olmayabilir.**
- SYN Scan, Nessusa gömülü olarak gelen TCP tarayıcısı, hedefteki açık TCP portlarını tayin etmek için kullanılır. SYN taraması, port taramalarını yönetmek için kullanılan popüler bir yöntemdir ve genelde TCP taramalarına göre biraz daha az zorla giriş yöntemini kullanır. Tarayıcı porta SYN paketi gönderir ve karşılığında SYN-ACK paketi bekler ve portun açık veya kapalı olduğunda karar verir.
- SNMP Scan, Nessusun hedefler üzerinde SNMP servislerinin bulunma durumunu taramak için yönlendirir. Nessus tarama esnasında alakalı SNMP ayarlarını tahmin etmeye çalışır. Eğer ayarlar kullanıcı tarafından “preferences” seçeneği altında sağlanırsa, bu Nessusun hedefi daha iyi taramasına ve daha detaylı denetim raporlarının üretmesine yardımcı olacaktır. Mesela, geriye dönen SNMP değişkenine ait versiyonunun

incelenmesiyle, açıklıkların varolma durumuna karar veren birçok Cisco router vardır. Bu bilgi bu tip denetimler için gereklidir.

- Netstat SSH Scan, bu seçenek lokal makine üzerinden netstatı kullanarak açık portları kontrol eder. Bu seçenek hedefe yapılacak olan SSH bağlantısı vasıtasıyla netstat komutunun erişilebilirliğine dayanır. Bu tarama Unix tabanlı sistemlerde kullanılmayı amaçlar ve kullanıcı adı-şifre onayı gerektirir.
- Netstat WMI Scan, bu seçenek lokal makine üzerinden netstatı kullanarak açık portları kontrol eder. Bu seçenek hedefe yapılacak olan WMI bağlantısı vasıtasıyla netstat komutunun erişilebilirliğine dayanır. Bu tarama Windows tabanlı sistemlerde kullanılmayı amaçlar ve kullanıcı adı-şifre onayı gerektirir.
- Ping Host, bu seçenek uzak hostların birçok portunun pinglenmesiyle, açık olup olmama durumuna karar verir.

v. Port Scan Options

- “default”, “default” kullanılması durumunda, Nessus yaklaşık 4605 ortak portu tarayacaktır.
- “all”, “all” kullanılması durumunda, Nessus 65535 portu tarayacaktır.
- Custom List, virgülle ayrılmış şekilde hazırlanmış olan portlar veya port aralıkları listesi vasıtasıyla, özel olarak belirlenen aralıklar taranabilir. Mesela, “21,23,25,80,110” yada “1-1024, 8080, 9000-9200”. “1-65535” yazılması durumunda bütün portlar taranır.

vi. Performance

- Max Checks Per Host, bu ayar Nessus tarayıcının bir seferde bir hosta yapacağı maksimum sayıdaki kontrolü belirler.
- Max Hosts Per Scan, bu ayar Nessus tarayıcının aynı anda maksimum sayıda hosta yapacağı kontrolü belirler.
- Network Receive Timeout(seconds), varsayılan olarak 5 saniyeye ayarlanmıştır. Bu süre, tersi bir plugin tarafından belirtilmediği sürece, Nessusun bir hosttan bekleyeceği tepkidir. Eğer yavaş bağlantılarla tarama yapılıyorsa bu süreyi daha yüksek saniyelere ayarlayabilir.
- Max Simultaneous TCP Sessions Per Host, bu ayar bir hosta kurulacak olan maksimum sayıdaki TCP bağlantısını belirler.
- Max Simultaneous TCP Sessions Per Scan, bu ayar bir taramada kurulacak olan maksimum sayıdaki TCP bağlantısını, taranacak olan host sayısına bakılmaksızın, belirler.

b. Credentials

i. Windows Credentials

Nessus Serverın Windows işletim sistemine sahip hostlarla ilgili daha fazla tarama sonucu sağlayabilmesi için SMB hesap bilgilerinin girilmesi gerekmektedir. Bu şekilde uzaktaki bir Windows hostuna ait bilgileri Nessus

rahatlıkla sağlayacaktır. Mesela, Admin yetkilerine sahip olan hesap bilgileri vasıtasıyla Nessus uzaktaki hostun önemli güvenlik yamalarını kullanıp kullanmadığını bildirebilir veya PCI DSS gibi önemli uyumluluk kurallarına uygunluğunu denetleyebilir. Nessus Windows NT, 2000, 2003, XP, Vista, 7 ve 2008 hostları için birçok güvenlik kontrolü barındırır. Eğer bir domain hesabı sağlanırsa daha tutarlı sonuçlar ortaya çıkacaktır.

ii. SSH Credentials

Nessus Serverın Unix tabanlı işletim sistemlerine sahip hostlarla ilgili daha fazla tarama sonucu sağlayabilmesi için SSH hesap bilgilerinin girilmesi gerekmektedir. Bu bilgiler sayesinde, yama denetimi ve uyumluluk kontrolü sağlanacaktır. Çoğu yapı uzaktan root erişimine izin vermediği için, “Elevate privileges with” seçeneğini kullanarak, “su” veya “sudo” tercih edilerek yetkiler yükseltilebilir.

iii. Oracle Settings

Bu seçenek vasıtasıyla özel olarak taranması istenen Oracle Serverlar taranabilir. Oracle SID belirtilerek tercih edilen Oracle server taranabilir. Aynı zamanda bilinen varsayılan hesapların güvenlik kontrolü yapılabilir.

iv. Kerberos Configuration

Uzaktaki bir hostu taramak için Kerberos kimlik bilgileri verilebilir.

v. Cleartext Protocol Settings

Eğer güvenli protokoller vasıtasıyla güvenlik kontrolleri yapılamıyorsa, kullanıcı Nessusu güvenli olmayan protokoller üzerinden tarama yapmaya zorlayabilir. “Cleartext protocol settings” seçeneği altında gerekli bilgiler girilerek bu işlem kullanılabilir. Bu seçenek için telnet, rsh ve rexec protokolleri kullanılır.

Varsayılan olarak, herhangi bir tarama profili ile alakalı olan parolalar şifrelenir. Eğer profil .nessus uzantısı ile kaydedilir ve başka bir Nessus servera aktarılsa, diğer Nessus server bu şifreyi çözemeyeceği gibi parolaları da kullanamaz.

Bu sorunu çözmek için, “ save credentials as clear text in policy” seçeneği kullanılabilir. Bu şekilde, profillerde kullanılan parolalar şifrelenmez ve başka Nessus Serverlar tarafından kullanılabilir.

Uyarı: Bu yöntemin kullanılması önerilmemektedir. Kullanıcı adları ve parolalar tarama raporları ve/veya mail yöntemi ile gönderilirse network üzerinde herhangi bir kullanıcı tarafından ele geçirilebilir.

c. Plugins

Daha önce belirtildiği üzere, Nessus Serverın daha performanslı çalışabilmesi ve istenilen sonuçların elde edilebilmesi için özel profiller oluşturulmalıdır. “Plugins” tercihi ile tarama yapılacak kapsama göre gerekli olanlar tercih edilmelidir. Pluginlerin yanlarında bulunan yuvarlaklar eğer sarı renk ise o pluginin seçili olduğu gösterir. Pluginler aile olarak kullanılabilceği gibi, bir ailenin içinden belirli pluginler de seçilebilir.

Uyarı: “Denial of Service” plugin ailesi, eğer “Safe Checks” tercihi ile kullanılmazsa, şirket networkünde kesintilere neden olabilir, aynı zamanda zarar vermeyecek önemli bileşenleri de vardır. İki tercih beraber kullanılarak zararlı pluginlerin kullanılmayacağını temin edebilirsiniz, yinede PROD ortamında bu plugin ailesini tercih etmeyiniz.

d. Preferences

Bu seçeneğin altında bulunan bileşenler vasıtasıyla, profillere daha fazla bilgi eklenerek taramalardan daha fazla sonuç elde edilebilir.

i. Database Compliance Checks

- Login, veritabanı için kullanıcı ismini belirtir.
- Password, verilen kullanıcı ismi için parolayı belirtir.
- DB Type, seçilecek veritabanı tipini belirtir. Desteklenen veritabanları, Oracle, Sql Server, MySql, DB2, Informix/DRDA, PostgreSQL dır.
- Database SID, denetlenecek olan veritabanının ID numarasını belirtir.
- Database port to use, veritabanının dinlediği portu belirtir.
- Oracle auth type, “NORMAL”, “SYSOPER” ve “SYSDBA” desteklenir.
- SQL Server auth type, Windows yada SQL desteklenir.

ii. Do not Scan Fragile Devices

Bu seçenek vasıtasıyla, tarama yüzünden servis dışı kalabilecek yazıcılar ve/veya Novell network hostlarının taraması engellenebilir. İş saatleri esnasında tarama yapılacaksa, bu seçeneğin kullanılması önerilir.

iii. Global Variable Settings

- Probe services on every port, her portta çalışan servisleri keşfetmeyi belirtir. Çok sık gözükmemesine rağmen, bazı servisleri durdurduğu gözlemlenmiştir.
- Do not log in with user accounts not specified in the policy, hesap kilitlenmelerini engellediğini belirtir.
- Enable CGI scanning, CGI kontrollerinin yapılacağını belirtir. Bu seçenek kullanılmazsa network denetim hızı oldukça yükselir.

- Network type, ne tür ip kullanıldığını belirtir. “public routable”, “private non-internet routable” ve “mixed” seçenekleri kullanılabilir. Eğer RFC1918 adresler kullanılıyorsa ve network içinde çok fazla sayıda router bulunuyorsa “mixed” tercih edilmelidir.
- Enable experimental scripts, experimental scriptlerin kullanılacağını belirtir. PROD ortamı tararken bu seçenek tercih edilmemelidir.
- Thorough tests (slow), pluginlerin daha fazla çalışacağını belirtir. Her plugin daha detaylı sonuç verecek şekilde çalışır. Daha iyi denetim sonuçları alınırken, network trafiği artabilir ve tarama networkü yavaşlatabilir.
- Report verbosity, raporda daha fazla detay verileceğini belirten seçenektir.
- Report paranoia, taramalar esnasında kusurların varlığını belirtir. “Paranoid” hedef hostun bir kusuru olduğu şüpheli bile olsa raporda belirtilir, “avoid false alarm” false positive alarm sayısını azaltır, “normal” iki seçeneğin ortasındaki tercihtir.
- Debug level, Nessus taramasıyla ilgili sorun çözerken, bu seçeneğin “1” olarak atanması, debugging in yardımcı olacağını belirtir.
- HTTP User-Agent, hangi tür browser kullanıldığını belirtir. Belirtilen seçeneği Nessus kullanarak, browser gibi davranır.
- SSL certificate to use, Nessus'un uzaktaki host ile iletişim kurmak için kullanabileceği client side sertifikayı belirtir.
- SSL CA to trust, Nessus'un kullanacağı CA (Certificate Authority) belirtir.
- SSL key to use, uzak host ile iletişim kurmak için kullanılacak olan SSL anahtarını belirtir.
- SSL password for SSL key, tanımlanan SSL anahtarını yöneten parolayı belirtir.

iv. HTTP Login Page

- Login page, uygulamanın kullanacağı login sayfasının URL'sini belirtir.
- Login form, form methodu için kullanılan “action” parametresini belirtir.
- Login form fields, onaylama parametrelerini belirtir.
- Re-authenticate delay (seconds), onay alma denemeleri arasındaki süre farkını belirtir.
- Check authentication on page, onaylama gereken korumalı web sayfasının URL'sini belirtir.
- Follow 30x redirections (# of levels), eğer web serverdan 30x yeniden yönlendirme kodu dönerse, Nessus'un bağlantıyı takip edip, etmeyeceğini belirtir.
- Authenticated regex, login sayfasında aranması istenilen regex örneğini belirtir. Mesela, “authentication successful!” yakalanırsa Nessus başarılı olmuştur.
- Invert test (disconnected if regex matches), login sayfasında aranması istenilen regex örneğini belirtir. Mesela, “authentication failed!” yakalanırsa Nessus başarısız olmuştur.

- Match regex on HTTP headers, onaylamanın durumunu öğrenmek için Nessusun HTTP Headerlarını kontrol ettiğini belirtir.
- Case insensitive regex, varsayılan olarak regex aramaları büyük-küçük harf duyarlıdır. Bu tercih ile duyarlılığın kaldırılacağını belirtir.

v. ICCP/COTP TSAP Addressing

SCADA taramaları için kullanılacak detayları belirtir.

vi. Login Configurations

Nessus tarayıcısının HTTP, NNTP, POP2, POP3 veya IMAP tararken kimlik bilgilerinin kullanılıp kullanılmayacağını belirtir. Kimlik bilgileri verilirse, Nessus daha geniş çapta zafiyet taraması yapacaktır.

vii. Modbus/TCP Coil Access

SCADA taramaları için kullanılacak detayları belirtir.

viii. Nessus SYN Scanner ve Nessus TCP Scanner

- Automatic (normal), hedef ile tarayıcı arasında firewall olup olmadığını belirtir.
- Disabled (softer), firewall bulma özelliğinin kapandığını belirtir.
- Do not detect RST rate limitation (soft), resetlerin ne sıklıkla ayarlandığını gözlemlene yeteneğinin kapatıldığını belirtir.
- Ignore closed ports (aggressive), portlar kapalı olsa dahi pluginlerin çalıştırılacağını belirtir. PROD ortamında kullanılmaması tavsiye edilir.

ix. News Server (NNTP) Information Disclosure

- From address, Nessus Serverin haber serverlarına mesaj göndereceği adresi belirtir.
- Test group name regex, tanımlanan bir adresten test mesajı alacak olan haber gruplarını belirtir.
- Max crosspost, isim eşleşme sayısına bakılmaksızın, test yazısını alacak olan serverların maksimum sayısını belirtir.
- Local distribution, bu seçenek tercih edilirse Nessus sadece lokal haber serverlarına mesaj göndermeye çalışır.
- No archive, bu seçenek tercih edilirse, Nessus göndereceği mesajların haber serverları tarafından arşivlenmemesini talep edecektir.

x. PCI DSS Compliance

PCI DSS uyumluluğunu denetlemek için kullanılır.

xi. Ping the Remote Host

- TCP ping destination port(s), TCP ping yoluyla kontrol edilecek portların listesini belirtir.
- Number of Retries (ICMP) , uzaktaki hostu pinglemek için kullanacağı deneme sayısını belirtir. Varsayılan olarak altı (6) dır.
- Do an applicative UDP ping (DNS, RPC...), spesifik olarak UDP bazlı çalışan uygulamalara yapılacak olan UDP pingini belirtir.
- Make the dead hosts appear in the report, pinglere cevap vermeyen hostların raporlarda kapalı olarak bildirileceğini belirtir.
- Log live hosts in the report, pinglere cevap veren hostların raporlarda açık olarak bildirileceğini belirtir.
- Test the local Nessus host, tarama esnasında Nessus Serverın bulunduğu hostun, taramaya eklenip eklenmeyeceğini belirtir.
- Fast network discovery, varsayılan olarak Nessusa gelen ping cevaplarının doğruluğunu sağlamak amacıyla, cevap veren tarafında transparan proxy yada load balancer olup olmadığını bulmak için ekstra kontrol yapılacağını belirtir. Seçilmezse bu kontrol yapılmaz.

xii. Port Scanner Settings

- Check open TCP ports found by local port enumerators, WMI yada netstat gibi uygulamalar bir portun açık olduğunu bildirirse, Nessusun o portu açık ilan edeceğini bildirir. Bu şekilde access control mekanizmalarının kullanıldığına karar verilir.
- Only run network port scanners if local port enumeration failed, eğer WMI yada netstat çalışmazsa sadece network port taramalarının çalışacağını belirtir.

xiii. SMB Registry: Start the Registry Service during the scan

SMB kayıtlarını her zaman çalıştırmayan hostlar için tarama gereksinimlerini kolaylaştıran servisi aktif hale getirmek için kullanılır.

xiv. SMB Scope

- Request information about the domain, lokal kullanıcılar yerine domain kullanıcılarının değerlendirileceğini belirtir.

xv. SMB use domain SID to enumerate users

Domaindeki kullanıcı isimlerini tersten araştırmak için kullanılacak olan SID aralığını belirtir. Varsayılan olarak bütün taramalar için kullanılması tavsiye edilir.

xvi. SMB use host SID to enumerate local users

Lokaldeki kullanıcı isimlerini tersten araştırmak için kullanılacak olan SID aralığını belirtir. Varsayılan olarak bütün taramalar için kullanılması tavsiye edilir.

xvii. SMTP Settings

- Third party domain, bu alanda belirtilen adresteki bütün kullanıcılara Nessusun spam mail göndereceğini belirtir. Bu adres, taranılan yada tarayan sistemin dışarısında olmalıdır. Aksi takdirde SMTP server engelleyecektir.
- From address, gönderenin adresini belirtir.
- To address, mailin gideceği kişi veya kişileri belirtir.

xviii. SNMP Settings

- Community name, SNMP community ismini belirtir.
- UDP port, SNMP servisinin çalıştığı UDP portunu belirtir. Varsayılan olarak 161 tir.
- SNMPv3 user name, SNMPv3 bazlı hesabın kullanıcı ismini belirtir.
- SNMPv3 authentication password, verilen kullanıcı isminin parolasını belirtir.
- SNMPv3 authentication algorithm, uzaktaki servisin desteğine göre MD5 veya SHA1 şifreleme algoritmasını belirtir.
- SNMPv3 privacy password, şifreli SNMP iletişimini korumak için kullanılan parolayı belirtir.
- SNMPv3 privacy algorithm, SNMP trafiği için kullanılacak olan şifreleme algoritmasını belirtir.

xix. Service Detection

Nessusun SSL bazlı servislerini nasıl test edeceğini kontrol eder. Bilinen SSL portlar (443), bütün portlar yada hiçbir port tarama seçenekleri kullanılabilir.

xx. Unix Compliance Check

Tenable security şirketinin hazırladığı .audit uzantılı dosyalar vasıtasıyla Unix tabanlı işletim sistemleri üzerinde uyumluluk kontrolü yapılır. Beş dosyaya kadar destekler.

xxi. Web Application Test Settings

“Enable web applicaiton tests” tercihi seçilerek kullanılır. Aşağıda ID numarası ve isimleri belirtilen pluginler üzerinden gerçekleştirilir :

- 11139 – SQL Injection (CGI abuses)
- 39465 – Command Execution (CGI abuses)
- 39466 – Cross-Site Scripting (CGI abuses: XSS)
- 39467 – Directory Traversal (CGI abuses)
- 39468 – HTTP Header Injection (CGI abuses: XSS)
- 39469 – Remote File Inclusion (CGI abuses)

Bileşenler şu şekildedir :

- Maximum run time (min), verilen bir web sitesinin bütün portlarına ve CGI larına uygulanacak testin dakika bazında süresini belirtir. Varsayılan süre 60 dakikadır.
- Send POST requests, “POST Request” testini geliştirilmiş web formları üzerinde yapılacağını belirtir. Eğer bu seçenek kullanılmazsa GET testleri gerçekleştirilir.
- Combinations of arguments values, HTTP isteklerinde kullanılan argüman değerlerinin kombinasyonlarını belirtir.
- HTTP Parameter Pollution, web uygulamaları testleri gerçekleşirken, filtreleme mekanizmalarını bypass etmek amacıyla, varolan değişkenlerin içerisine ekstra bilgi ekleyerek farklı parametreler kullanılacağını bildirir.
- Stop at first flaw, Nessus Serverın port veya CGI başına ortaya çıkabilecek kusurlar karşısında nasıl davranacağını belirtir.
- Test Embedded web servers, gömülü web serverları genelde statiktir ve üzerlerinde özelleştirilebilen CGI scriptleri bulunmaz. Bununla beraber, web uygulama testi esnasında servis dışı kalabilir veya cevap vermeyebilir. Bu seçenek, gömülü web serverları diğer web serverlardan ayırarak test yapılacağını belirtir.

- URL for Remote File Inclusion, bu test esnasında Nessus tarayıcı internet üzerinden güvenli bir dosya indirir ve hedef hosta gönderir. İnternetin bulunmadığı durumlarda, içeride saklanan bir dosyanın kullanımı daha tutarlı bir test olmasına yardımcı olur. Bu seçenek ile bu testin aktif hale gelmesi sağlanır.

xxii. Web Mirroring

- Number of pages to mirror, yansıtılacak sayfaların sayısını belirtir.
- Maximum depth, her başlangıç sayfası için Nessusun takip edeceği bağlantıların sınırını belirtir.
- Start page, test edilecek ilk başlangıç sayfasını belirtir.
- Excluded items regex, taranacak web sitesinin ulaşılması istenmeyen yerlerini belirtir.
- Follow dynamic pages, tercih edilirse Nessusun dinamik bağlantıları takip edeceğini belirtir.

xxiii. Windows Compliance Check

Tenable security şirketinin hazırladığı .audit uzantılı dosyalar vasıtasıyla Windows tabanlı işletim sistemleri üzerinde uyumluluk kontrolü yapılır. Beş dosyaya kadar destekler.

xxiv. Windows File Contents Compliance Checks

Tenable security şirketinin hazırladığı .audit uzantılı dosyalar vasıtasıyla Windows tabanlı işletim sistemleri üzerinde spesifik tipteki içeriklerin denetlemesini sağlar, kurum ve 3. Parti yazılımlarla uyumluluğunu kontrol eder.

7. Kullanıcılar

Nessus tarayıcısının arayüzünü yönetecek olan kullanıcıların bulunduğu kısımdır. “Users” tuşuna basılarak bu bölüme geçilebilir. “Users” bölümünün ekran görüntüsü aşağıdaki gibidir :



Name	Username	Role	Last Login
admin	admin	Administrator	Nov 20, 2009 24:49
figlet	figlet	User	Never Logged In

Bu bölümde yeni kullanıcı eklenebilir, varolan kullanıcıların bilgileri ve hakları değiştirilebilir veya varolan kullanıcılar silinebilir.