ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/nessus-kullanim-kitapcigi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Nessus%20Kullan%C4%B1m%20Kitap%C3%A7%C4%B1%C4%9F%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

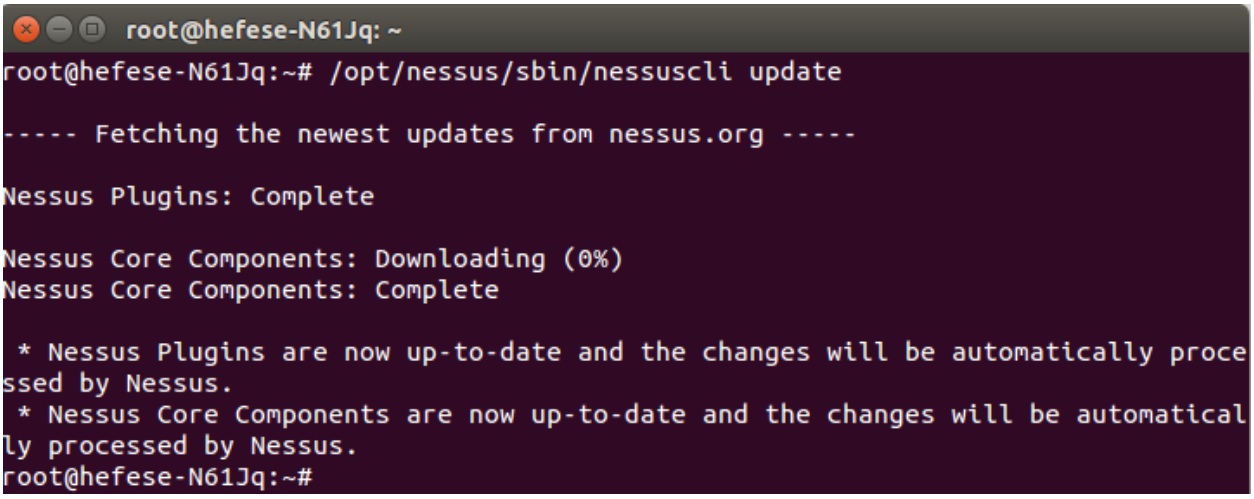
Nessus’da oluşturulacak tarama profilleri vasıtasıyla bütün bir network veya belirli hostlar taranabilir, güvenlik açıklıkları keşfedilebilir.

(Page 4)

2)

Nessus’a ait olan pluginler bir taramanın davranışlarını ve kapsamını belirlemek için kullanılır. Tarama sonuçlarının güncel olması açısından sistemde yüklü plugin’ler güncelleştirilmelidir. Plugin’ler varsayılan olaraktan 24 saatte bir otomatikmen güncelleştirilmektedir. Dilenildiği takdirde güncelleştirme manuel olarak aşağıdaki komut ile yapılabilmektedir:

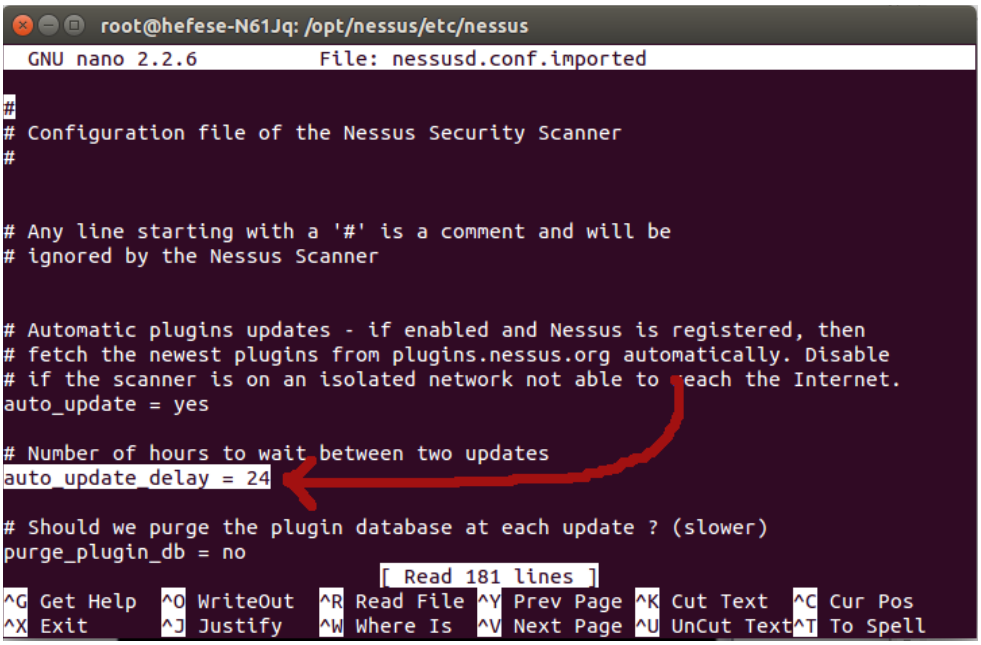
> /opt/nessus/sbin/nessuscli update



Nessus'un 24 saat ayarını kısaltmak için aşağıdaki adımlar takip edilmelidir:

> cd /opt/nessus/etc/nessus

> nano nessusd.conf.imported



24 saatlik süreyi dilenilen süreye çekebilirsiniz.

(Page 4-5)

3)

Tarama Profilleri (Policy)

Nessus ile tarama yapmak için öncelikle tarama profilleri oluşturulmalıdır. Bir profil oluşturulmazsa ve o profile kapsam tanımlaması yapılmazsa taramalarda zaman ve performans kayıpları, hatta nitelikli sonuçların elde edilememesi gibi sorunlarla karşılaşılabilir.

(Page 10)

4)

Tarama profili oluşturabilmek için Nessus arayüzündeki Policy butonuna tıklanılmalıdır. Tarama profilinin kapsamını belirlemek için ise Policies > Settings dizini altındaki sol tarafta sıralı BASIC, DISCOVERY, ASSESSMENT, REPORT ve ADVANCED menülerine tıklanılmalı ve istenilen şekilde ayarlar yapılandırılmalıdır. Oluşturulan tarama profili ile tarama yapabilmek için ise New Scan butonuna tıklanılmalı ve ardından template'lerin en aşağısında yer alacak olan oluşturduğumuz tarama profiline tıklanılmalıdır.

(Benim Notum Bu)

5)

Credentials

i) Windows Credentials

Nessus'un Windows işletim sistemine sahip hostlarla ilgili daha fazla tarama sonucu sağlayabilmesi için SMB hesap bilgilerinin Nessus'a girilmesi gerekmektedir *(Nasıl yapılacağı birazdan bahsedilecektir)* . Mesela, admin yetkilerine sahip olan hesap bilgileri vasıtasıyla Nessus uzaktaki hostun önemli güvenlik yamalarını kullanıp kullanmadığını denetleyebilir ve daha başka tutarlı sonuçlar ortaya çıkarabilir.

ii) SSH Credentials

Nessus'un Unix tabanlı işletim sistemlerine sahip hostlarla ilgili daha fazla tarama sonucu sağlayabilmesi için uzak sistemin SSH hesap bilgilerinin Nessus'a girilmesi gerekir *(Nasıl yapılacağı birazdan bahsedilecektir)*. Bu bilgiler sayesinde Nessus uzak sistem için yama denetimi yapabilir.

iii) Oracle Settings

Nessus'a özel olarak uzak sistemdeki bir veritabanını (mesela Oracle'ı, MySQL'i, PostgreSQL'i, DB2'yu, SQL Server'ı...) taratılabilmektedir. Böylece bilinen varsayılan hesapların güvenlik kontrolleri yapılabilir.

NOT:

Windows Credentials'larını Nessus'a girmek için New Scan butonuna tıkla. Sonra Credentialed Patch Audit template'ini seç. Ardından Policies > Credentials dizini altına geç ve Windows menüsüne basarak bilgileri girebilirsin.

SSH Credentials'larını Nessus'a girmek için New Scan butonuna tıkla. Sonra Credentialed Patch Audit template'ini seç. Ardından Policies > Credentials dizini altına geç ve SSH menüsüne basarak bilgileri girebilirsin.

Spesifik bir veritabanını Nessus'a taratmak için New Scan butonuna tıkla. Sonra Credentialed Patch Audit template'ini seç. Ardından Policies > Credentials dizini altına geç ve Database menüsünün içindeki Database sekmesine tıkla. Gelen içerikten dilediğin veritabanını seçebilir ve login bilgilerini girebilirsin *(SID diye tabir edilen uzak sistemdeki veritabanının ID bilgisi login bilgileri ile beraber girilmek zorundadır).*

(Page 13-14)

6)

Kimlik bilgileri verilirse Nessus daha geniş çapta zafiyet taraması yapacaktır.

(Page 17)