

# Nessus ve Nikto

Gökhan Alkan, Ağustos 2009, WGT E-Dergi 1. Sayı

---

## Giriş

Hemen hemen bütün güvenlik denetimlerinin olmaz ise olmaz adımı hedef sistemler üzerinde keşif gerçekleştirmektir. Hem keşif gerçekleştirmek hem de zafiyet taraması için açık kaynak kod dünyasında bu işlem için kullanılan en popüler araçlardan bir tanesi şüphesiz Nessus'dur.

Hem ticari hem de ücretsiz sürümleri ile bir çok kişi tarafından yaygın bir şekilde kullanılmaktadır.

Nikto Sullo tarafından geliştirilmiş açık kaynak kodlu, ufak ancak hızlı çalışan bir web keşif uygulamasıdır. Kurulum gerektirmeden kolay bir şekilde kullanılabilir olması özellikle web güvenlik denetimlerinde tercih edilmesine sebep olmuştur.

Bu yazıda öncelikle Nikto uygulamasının nasıl kullanılabileceğini ardından, Nessus ile entegre biçimde web güvenlik denetimlerinde nasıl kullanılacağı anlatılmaktadır.

Burada anlatılanlar tamamen Unix/Linux sistemlere özeldir. Nessus'un Nikto uygulamasını kullanmak için kullandığı "nikto.nasl" plugini Windows sistemler üzerinde çalışan Nessus, Nikto ile kullanılamaz. Bu makalede RedHat 5.3, Nessus 4.0.1 ve Nikto 2.03 sürümü kullanılmıştır.

## Nikto Kullanımı

Nikto kullanımı esnasında SSL bağlantılarını gerçekleştirmek için "Net\_SSLeay.pm" perl modülü kullanılmaktadır. Bu modülün sisteme kurulması için aşağıdaki adımları sırası ile uygulanması gerekmektedir.

```
# cd /tmp
# wget http://search.cpan.org/CPAN/authors/id/F/FL/FLORA/Net\_SSLeay.pm-1.30.tar.gz
# tar -zxvf Net_SSLeay.pm-1.30.tar.gz
# cd ./Net_SSLeay.pm-1.30
# perl Makefile.PL
# make
# make install
```

Gerekli modülün sisteme kurulmasının ardından Nikto, <http://www.cirt.net/> adresinden temin edilmelidir. Nikto yazılımının kurulumu için aşağıdaki adımları sırası ile uygulanmalıdır.

```
# cd /tmp
# wget http://www.cirt.net/nikto/nikto-current.tar.gz
# tar -zxvf nikto-current.tar.gz
```

```
# cp -R nikto /opt/  
#
```

Nikto, LibWhisker kütüphanesi temel alınarak geliştirilmiş bir uygulamadır. (<http://www.wiretrip.net/rfp/lw.asp>). Gerekli kütüphane Nikto çalıştırılacak dizine temin edilmelidir.

```
# /opt/nikto  
# wget http://www.wiretrip.net/rfp/libwhisker/LW.pm  
# chmod 755 LW.pm
```

Nikto yazılımı çalıştırmadan önce kurulumun bulunduğu dizin PATH çevresel değişkeni içerisinde bulunması gerekmektedir. PATH çevresel değişkenini öğrenmek için echo komutu kullanılabilir.

```
# echo $PATH  
/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
```

Yukarıdaki çıktıda görüldüğü gibi Nikto yazılımının kurulum dizini PATH çevresel değişkeni içerisinde bulunmamaktadır, eklemek için export komutu kullanılabilir.

```
# export PATH=$PATH:/opt/nikto/  
# echo $PATH  
/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/opt/nikto:/opt/nikto/
```

Nikto kurulum dizininin PATH çevresel değişkenine eklenmesinin ardından nikto yazılımı güncellenerek çalıştırılmalıdır. Nikto yazılımı çalışma esnasındaki değerleri "-config" parametresi ile belirtilen dosya içerisinden almaktadır. Kaynak kod ile birlikte "config.txt" adında örnek bir dosya gelmektedir. Bu dosyanın içeriği kullanıma uygun olarak değiştirilmeli ve yine uygun bir dizine kopyalanmalıdır. Nikto çalışması esnasında bu dosyanın içeriğini okuyacaktır.

```
# cp /tmp/nikto/config.txt /etc/config  
# vi /etc/config  
  EXECDIR=/opt/nikto  
#
```

Nikto yazılımı port tarama uygulaması için "nmap" yazılımını kullanmaktadır. Bunun için nmap yazılımının sistemde kurulu olması ve çalıştırılabilir yolunun Nikto yapılandırma dosyasına eklenmesi gerekmektedir. RHEL sistemler üzerinde nmap kurulumu için;

```
# yum install nmap
```

Nmap uygulamasının çalıştırılabilir tam yolunu öğrenmek için ise which nmap komutu kullanılabilir.

```
# which nmap
/usr/bin/nmap
# vi /etc/config
NMAP=/usr/bin/nmap
```

Ardından Nikto güncellemesi gerçekleştirilmelidir.

```
# nikto.pl -config /etc/config -update
+ Retrieving 'db_outdated'
```

Nikto ile ilgili modül ve kütüphanelerin sistem kurulmasının ardından nikto çalışması kontrol edilmelidir. En basit kullanımı için:

```
# nikto.pl -config /etc/config -h 192.168.1.2 -p 80
```

Daha fazla ayrıntı için komut --help parametresi ile çalıştırılarak ilgili seçenekler kullanılabilir yada <http://cirt.net/nikto2-docs> adresi ziyaret edilebilir.

## Nessus ile Entegre Kullanımı

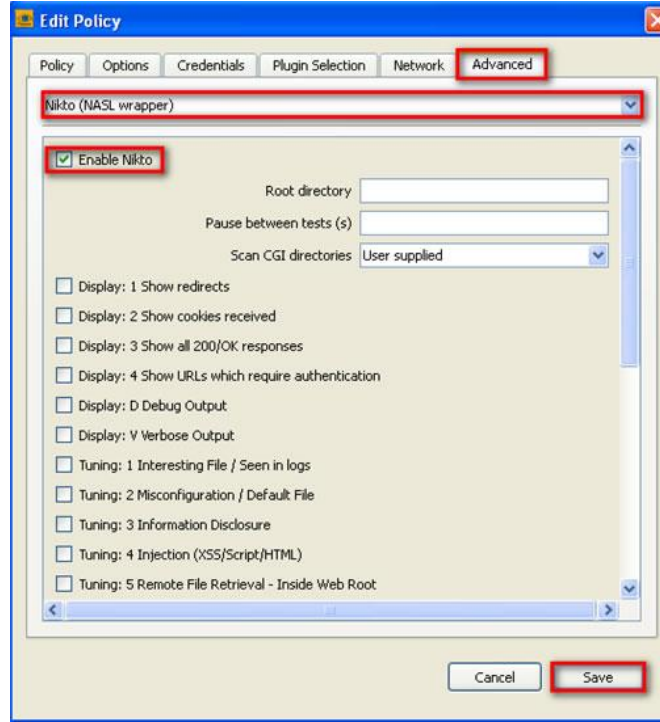
Nessus'un nikto ile çalışmasını sağlayan nessus pluginin "nikto.nasl" sistemde var olduğundan emin olunmalıdır. Plugin dizini altında 14260 numarasına sahip nikto.nasl plugini görülebilir.

```
# ls -al /opt/nessus/lib/nessus/plugins/nikto.nasl
-rw-r--r-- 1 root root 10195 Jul 10 14:04 /opt/nessus/lib/nessus/plugins/nikto.nasl
```

Ardından Nessus'un pluginleri yeniden çağırması için nessusd -R parametresi ile çağrılmalıdır ve nessus yeniden başlatılmalıdır.

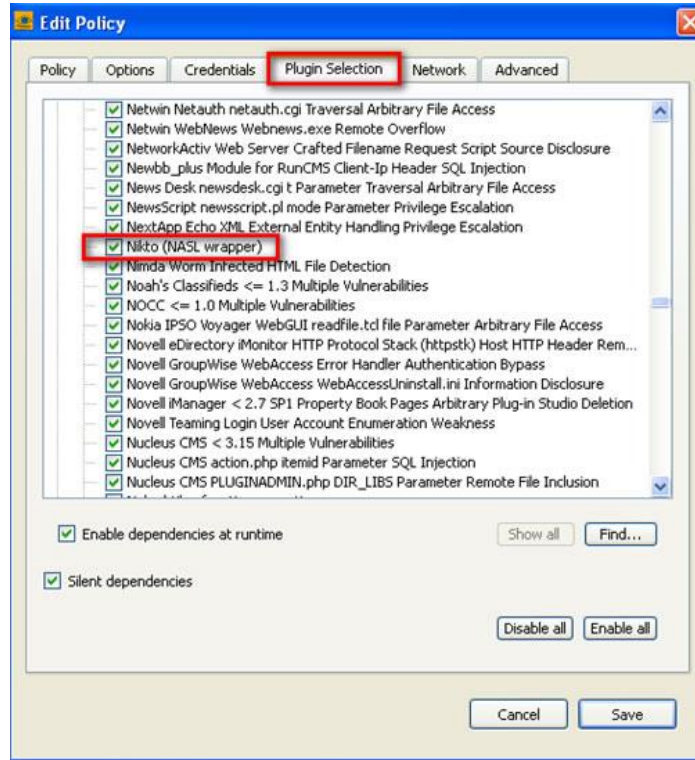
```
# nessusd -R
# /etc/init.d/nessusd restart
```

Gerekli işlemlerin gerçekleştirilmesinin ardından Nessus arayüzünden ilgili politika oluşturularak Nikto kullanımı etkin hale getirilmelidir. Bu işlem Advanced -> Nikto (NASL wrapper) -> Enable Nikto ile gerçekleştirilebilir. Bu durum Şekil 1'de gösterilmiştir. İlgili mönüden tarama esnasında kullanılmak istenen seçenekler aktif hale getirilmelidir.



Şekil 1: Nikto Uygulamasının Nessus ile Entegre Kullanımı - 1

Aynı şekilde Nessus ara yüzünden "CGI abuses" seçeneği altında Nikto (NASL wrapper) ile görüntülenmektedir. Bu durum Şekil 2'de görüntülenmektedir.



Şekil 2: Nikto Uygulamasının Nessus ile Entegre Kullanımı - 2