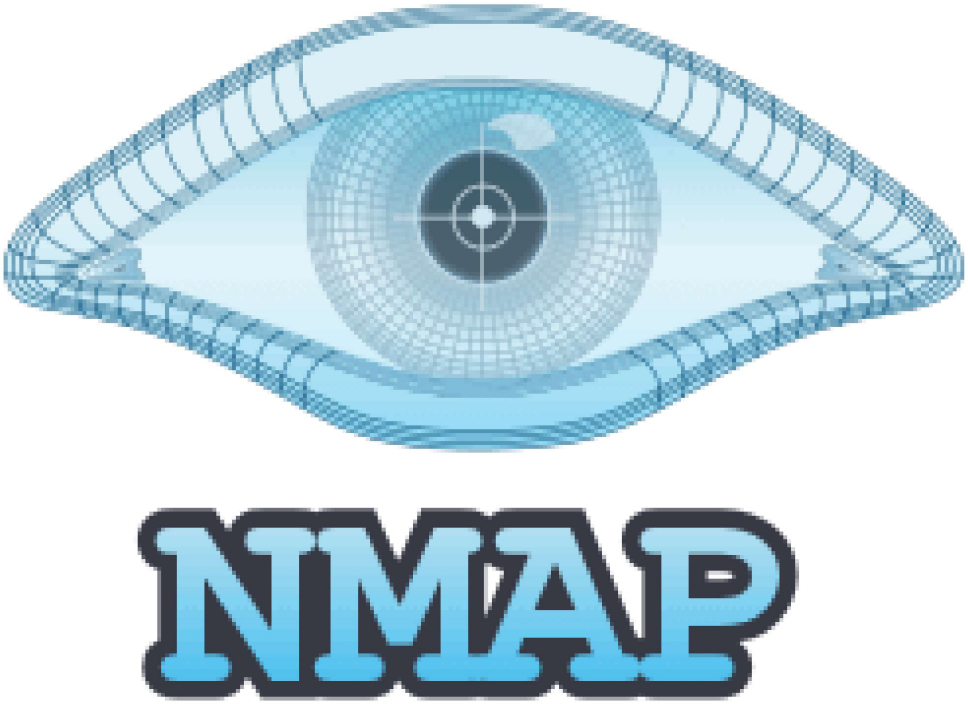
NMAP Komutu ve Kullanımı

Yazar: siberoloji Kategori: Nasıl? Yazdır: PDF

20 Mayıs 2017 tarihinde yayımlandı.

Bu yazıda, her Linux kullanıcısının kullanmayı bilmesi gerektiğini düşündüğüm nmap komutu örnekler ile ele alınmıştır.



Merhaba, bu yazıda her Linux kullanıcısının mutlaka kullanmayı öğrenmesi gereken bir yazılım olan `nmap` programından bahsetmek istiyorum. Belki de adını duymuşsunuzdur ancak bu yazıda, bir kaç örnekle birlikte kullanımını göstermek istiyorum.

nmap Nedir?

Network Mapper yani ağ haritasını çıkaran program olarak bilinen `nmap` , detaylarına inildiğinde çok güçlü bir ağ yönetim yardımcısıdır. Bünyesinde barındırdığı bir çok tarama seçeneği ile ağda bulunan cihazların keşfedilmesini sağlar.

Benzer Yazılar

Ubuntu 16.04.1 üzerine phpBB forum yazılımının 3.2 sürümünün kurulumu

su ve sudo Hakkında Bir Çalışma

Linux Strings Komutu Kullanımı

Nmap Script Engine adı verilen scriptleri kullanarak, ağda bulunan cihazların zafiyetlerini keşfetme ve gerekli önlemleri alma imkanı verir. Komut satırından `nmap` komutuyla kullanabileceğiniz gibi, GUI sürümü olan `zenmap` programını da kullanabilirsiniz. Bu yazıda komut satırından kullanım gösterilecektir.

nmap Kurulum

Nmap programı hemen hemen tüm dağıtımların paket depolarında yer almaktadır. Kurulum için `apt` komutu ile devam edelim.

```
sudo apt install nmap
```

İşte bu kadar. `nmap` bilgisayarınıza kuruldu. Komut satırında `nmap --help` komutunu verdiğinizde, oldukça detaylı kullanım parametrelerini görebilirsiniz. Bu yazıda hepsinin detayına girmemiz mümkün olmadığından çoğunlukla kullanılanları göreceğiz.

nmap Tarama Adımları

1. nmap Varsayılan Kurallar

- Siz herhangi bir tarama türü belirtmezseniz `TCP` taraması yapılır.
- Siz farklı bir aralık belirtmezseniz, bir IP adresi üzerinde en çok kullanılan 1000 port taranır.
- `nmap` önce bir IP adresine `ping` sinyali gönderir ve cevap alamaz ise o IP kapalı olarak kabul eder. Oysa, IP adresinde çalışan bir Firewall varsa `ping` sinyaline cevap vermemeye ayarlanmış olabilir. Ping taraması yapmadan her IP adresini açık kabul etmek için `-Pn` parametresini kullanmalısınız.

2. nmap Parametreleri

- `-sn` : Port taraması **yapma** anlamına gelir.
- `-n` : DNS Çözümlemesi **yapma** anlamına gelir.
- `-v` , `-vv` , `-vvv` : Ekrana gösterilecek detayları arttırır.

- `-F` : Daha hızlı tarama yapar. Daha **az** sonuç bulur.
- `-sS` :Syn Taraması Yapar
- `--reason` : Bulduğu bir sonucun sebebini gösterir.
- `--open` : Sadece açık Portları gösterir.
- `-p-` : Bir IP üzerinde bulunması muhteme 65535 portun hepsini tarar.
- `-sV` : Açık portta çalışan servisin ne olduğunu bulmaya çalışır. `-sC` ile birlikte kullanılırsa işe yarar.
- `-sC` : `-sV` ile versiyon tespiti yapılırken `nmap` scriptlerini kullanır.
- `-p` : Sadece bu parametreden sonra belirtilen portları tarar.

3. Taranacak IP Aralığı

Taramamıza başlamadan önce, hangi IP aralığını tarayacağımızı tespit etmeliyiz. Tabii ki bizim de üyesi bulunduğumuz bir ağı taramamız gereklidir. `ifconfig` komutuyla bilgisayarımızın IP adresini öğrenelim.

```
ifconfig

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3324 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3324 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:296929 (296.9 KB)  TX bytes:296929 (296.9 KB)

wlp3s0    Link encap:Ethernet  HWaddr 28:c2:dd:a6:af:5b
          inet addr:192.168.1.112  Bcast:192.168.1.255  Mask:255.255.2
          inet6 addr: fe80::702d:ec16:24d0:905/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25653 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18391 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9525019 (9.5 MB)  TX bytes:2675265 (2.6 MB)
```

Komut çıktısında görüldüğü gibi `wlp3s0` cihazımız, IPv4 formatında `192.168.1.112` adresini kullanmaktadır. O zaman, bizimle aynı ağda bulunan cihazlar, bağlı bulundukları DHCP Sunucudan büyük ihtimalle `192.168.1.1` ile `192.168.1.255` aralığında IP adresleri almıştır.

> **NOT:**
> Akıllı ağ yöneticileri bu IP adresini elle (manual) ayarlarlar ve

> yukarıda varsayılan önermeden kurtulurlar.

Bu durumda tarayacağımız IP aralığını `nmap` komutuna `192.168.1.1-255` olarak verebileceğiniz gibi CIDR gösterimi ile `192.168.1.0/24` şeklinde de verebiliriz.

4. nmap Tarama Adımları

Bu noktadan sonra artık tarama yapabiliriz. Bu tarama işlemini de 3 safhada ele almalısınız. Her bir safhada bulacağınız bilgiler, bir sonraki safhada kullanılacaktır.

1. IP Tarama:

Bağlı bulunduğunuz ağdaki cihazları ve aldıkları IP adresleri öğrenmek için yapılır.

1. Port Tarama:

Ağda bulunan IP adreslerini kullanarak, bu adreslerde hangi portların açık olduğunu bulmak için kullanılır.

1. Portlarda Servis Tarama:

Portlarda bulunan servislerin neler olduğunu tespit etmek için kullanılır.

4.1. nmap ile Açık IP adreslerini Öğrenme

İlk taramamızı, yukarıda belirttiğimiz 1.safhayı gerçekleştirmek için yapalım.

```
nmap -sn -n -v --open 192.168.1.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2017-05-20 22:25 +03
Initiating Ping Scan at 22:25
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 22:25, 20.49s elapsed (256 total hosts)
Nmap scan report for 192.168.1.1
Host is up (0.40s latency).
Nmap scan report for 192.168.1.100
Host is up (0.086s latency).
Nmap scan report for 192.168.1.101
Host is up (0.46s latency).
Nmap scan report for 192.168.1.102
Host is up (0.72s latency).
Nmap scan report for 192.168.1.103
Host is up (0.39s latency).
```

```
Nmap scan report for 192.168.1.104
Host is up (0.37s latency).
Nmap scan report for 192.168.1.112
Host is up (0.000070s latency).
Nmap scan report for 192.168.1.151
Host is up (0.0070s latency).
Nmap scan report for 192.168.1.169
Host is up (0.33s latency).
Nmap scan report for 192.168.1.184
Host is up (0.59s latency).
Nmap scan report for 192.168.1.199
Host is up (0.0056s latency).
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (11 hosts up) scanned in 20.49 seconds
```

Gördüğünüz gibi tarama sonucunda, ağımızda 11 adet IP adresi bulunmuştur. Acaba bu IP adreslerinde hangi Portlar açık? Bu sorunun cevabına bakalım.

4.2. nmap ile Açık Portları Öğrenme

`nmap` komutuna bu IP adreslerini tek tek verebileceğiniz gibi, aralık belirterek Port taraması da yapabilirsiniz. Biz burada basit olarak açık IP adreslerinden sadece 1 tanesini seçelim ve o IP adresinin varsayılan 1000 portunu tarayalım. Zaten `ifconfig` komutuyla kendi IP adresimizi öğrenmiştik. Onu seçmemeye dikkat edin. İsterseniz onu da (kendinizi) tarayabilirsiniz.

Aşağıda, `SYN` taraması kullanıldığından, başında `sudo` komutu vermeliyiz çünkü SYN taraması normal kullanıcıların yapabileceği bir tarama değildir. Diğer parametrelerin ne anlama geldiğini yukarıda açıklamıştık. Bu komutun ne yapacağını açıkça yazalım ki anlaması kolay osun.

> 192.168.1.169 IP adresinde bulunan varsayılan 1000 portu, Ping Kontrolü yapmadan (`-Pn`), DNS çözümlemesi yapmadan (`-n`), SYN taraması ile (`-sS`)araştır ve ekrana açık bulunan portları (`--open`), sebebiyle birlikte (`--reason`) yazdır. İşlemin devam etme durumunu göster (`-v`)

</>

```
sudo nmap -Pn -sS -n -v --reason --open 192.168.1.169

Nmap scan report for 192.168.1.169
Host is up, received arp-response (0.0024s latency).
Not shown: 992 closed ports, 1 filtered port
Reason: 992 resets and 1 no-response
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
```

```
80/tcp   open  http         syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
1001/tcp open  unknown      syn-ack ttl 64
1900/tcp open  upnp         syn-ack ttl 64
MAC Address: 84:16:F9:FA:24:AD (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 32.60 seconds
           Raw packets sent: 1398 (61.496KB) | Rcvd: 1359 (54.388KB)
```

Çıktı sonucunda, yukarıda bulunan açık Portlar görülmektedir. Yanlarında Service sütününda bir takım servislerin açık bulunduğunu görmekteyiz. Şimdi bu servislerin detaylarını bulmaya çalışalım.

4.3. nmap ile Servis Versiyon Taraması

Bu örnekte, **192.168.1.169** IP adresinde bulunan açık Portlarda, **SYN** paketleri ile **Versiyon** Taraması yapılmaktadır.

```
sudo nmap -sS -sV -sC -n -v -p 21,53,80,139,445,1001,1900  192.16

Host is up (0.0040s latency).
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.0.8 or later
53/tcp   open  domain      dnsmasq 2.67
| dns-nsid:
|_  bind.version: dnsmasq-2.67
80/tcp   open  http        TP-LINK TD-W8968 http admin
| http-methods:
|_  Supported Methods: GET POST
|_http-title: Site doesn\'t have a title (text/html; charset=utf-8).
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
1001/tcp open  unknown
1900/tcp open  upnp        Portable SDK for UPnP devices 1.6.19 (Linux
```

Komutun çıktısının ilk bölümü yukarıdaki gibidir. Bu çıktıdan, açık portlarda çalışan servisler ve **Versiyon** bilgisini görebiliriz. Son olarak yaptığımız `nmap` taramasının sonucunun ikinci bölümüne bakalım.

```
Host script results:
| nbstat: NetBIOS name: ADSL ROUTER, NetBIOS user: <unknown>, NetBIOS
| Names:
```

```
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   ADSL ROUTER<00>       Flags: <unique><active>
|   ADSL ROUTER<03>       Flags: <unique><active>
|   ADSL ROUTER<20>       Flags: <unique><active>
|   WORKGROUP<00>         Flags: <group><active>
|   WORKGROUP<1d>         Flags: <unique><active>
|_  WORKGROUP<1e>         Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2017-05-20T23:35:58+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: share (dangerous)
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn\'t support SMBv2 protocol
```

Yukarıdaki ifadelere benzer sonuçları, siz kendi taramalarınızda da bulabilirsiniz. Burada yer alan çıktıda, `Samba 3.0.14a` kullanıldığı ve bu servisin `guest` misafir kullanıcı işlemlerine müsaade ettiği `authentication_level: share (dangerous)` satırıyla bize bildirilmektedir.

Sistem ve ağ yöneticisi olarak gerekli önlemleri almanız gerektiğini `nmap` komutuyla basitçe göstermiş olduk.

nmap ağ tarama nmap kullanım nmap kurulum 16.04.1

Yorumlar Topluluk Gizlilik Politikası Oturum Açın

1

Öner 3 Tweet Gönder Paylaş

En İyiye Göre Sırala

Tartışmaya katıl…

ŞUNUNLA OTURUM AÇIN

YA DA BİR DİSQUS HESABI AÇIN ?

Ad

Ze Us • 2 yıl önce

Harika anlatım teşekkürler.

^ | v • Yanıtla • Paylaş ›

Muhammed Ötün • 4 yıl önce

nmap in başka kullanım alanlarıda var mı ?

^ | v • Yanıtla • Paylaş ›

Bu yorum silinmiş.

UnKnow ➚ Guest • 2 ay önce

Ddos kısmı nasıl oluyo

^ | v • Yanıtla • Paylaş ›

Deha Berkin Bir ➚ UnKnow • 2 ay önce

dalga geçtim aknsdkansdknd

^ | v • Yanıtla • Paylaş ›

Onur Tuncel • 4 yıl önce

Muhteşem teşekkürler

^ | v • Yanıtla • Paylaş ›

Mehmet Bbrl • 4 yıl önce

Mükemmel bir anlatim şahane