NMAP BÖLÜM 16-18

Chapter 16. Ndiff Reference Guide (Bölüm 16. Ndiff Referans Kılavuzu)

İçindekiler

Description (Açıklama)

ndiff - Nmap taramalarının sonuçlarını karşılaştırmak için yardımcı program

`ndiff` [*<options>*] { *<a.xml>* } { *<b.xml>* }

Ndiff, Nmap taramalarının karşılaştırılmasına yardımcı olan bir araçtır. İki Nmap XML çıktı dosyasını alır ve aralarındaki farkları yazdırır. Gözlemlenen farklar şunlardır:

- Ana bilgisayar durumları (örn. yukarıdan aşağıya)
- Bağlantı noktası durumları (örn. açıktan kapalıya)
- Hizmet sürümleri (-sV'den)
- İşletim sistemi eşleşmeleri (-O'dan)
- Komut dosyası çıktısı

Ndiff, standart diff yardımcı programı gibi, bir seferde iki taramayı karşılaştırır.

Options Summary (Seçenekler Özet)

`-h`, `--help` ⇒ Bir yardım mesajı gösterin ve çıkın.

`-v`, `--verbose` ⇒ Yalnızca değişenleri değil, tüm ana bilgisayarları ve bağlantı noktalarını çıktıya dahil edin.

`--text` ⇒ Çıktıyı insan tarafından okunabilir metin biçiminde yazın.

`--xml` ⇒ Çıktıyı makine tarafından okunabilir XML biçiminde yazın. Belge yapısı dağıtımda bulunan ndiff.dtd dosyasında tanımlanmıştır.

Diğer tüm bağımsız değişkenler Nmap XML çıktı dosyalarının adları olarak alınır. Tam olarak iki tane olmalıdır.

Example (Örnek)

Farklı seçenekler kullanan iki Nmap taramasının çıktılarını karşılaştırmak için Ndiff'i kullanalım. İlkinde, hız için daha az bağlantı noktası tarayan hızlı bir tarama (-F) yapacağız. İkincisinde, daha büyük varsayılan bağlantı noktası kümesini tarayacağız ve bir NSE betiği çalıştıracağız.

```
# nmap -F scanme.nmap.org -oX scanme-1.xml
# nmap --script=html-title scanme.nmap.org -oX scanme-2.xml
$ ndiff -v scanme-1.xml scanme-2.xml
-Nmap 5.35DC1 at 2010-07-16 12:09
+Nmap 5.35DC1 at 2010-07-16 12:13

 scanme.nmap.org (64.13.134.52):
 Host is up.
-Not shown: 95 filtered ports
+Not shown: 993 filtered ports
 PORT      STATE  SERVICE VERSION
 22/tcp    open   ssh
 25/tcp    closed smtp
 53/tcp    open   domain
+70/tcp    closed gopher
 80/tcp    open   http
+|_ html-title: Go ahead and ScanMe!
 113/tcp   closed auth
+31337/tcp closed Elite
```

Değişiklikler satır başında - veya + ile işaretlenir. Çıktıdan -F hızlı tarama seçeneği olmadan yapılan taramanın iki ek bağlantı noktası bulduğunu görebiliriz: 70 ve 31337. Html-title betiği 80 numaralı port için bazı ek çıktılar üretmiştir. Port sayılarından, hızlı taramanın 100 portu (95 filtrelenmiş, 3 açık ve 2 kapalı), normal taramanın ise 1000 portu (993 filtrelenmiş, 3 açık ve 4 kapalı) taradığı sonucunu çıkarabiliriz.

Ndiff'in -v (veya --verbose) seçeneği, 22 ve 25 gibi değişmeyen portları bile göstermesini sağladı. v olmasaydı, bunlar gösterilmeyecekti.

Output (Çıktı)

İki çıktı modu vardır: metin ve XML. Metin çıktısı varsayılandır ve --text seçeneği ile de seçilebilir. Metin çıktısı Nmap'in normal terminal çıktısının birleştirilmiş bir farkını andırır. Her satırdan önce değişip değişmediğini ve nasıl değiştiğini gösteren bir karakter gelir. - satırın ilk taramada olduğu ancak ikinci taramada olmadığı anlamına gelir; + ise ikinci taramada olduğu ancak ilk taramada olmadığı anlamına gelir. Değişen bir satır - çizgisi ve ardından + çizgisi ile gösterilir. Değişmeyen satırların önünde bir boşluk bulunur.

Örnek 16.1 metin çıktısına bir örnektir. Burada, photos-cache-snc1.facebook.com ana bilgisayarındaki 80 numaralı bağlantı noktası bir hizmet sürümü (lighttpd 1.5.0) kazanmıştır. 69.63.179.25 adresindeki ana bilgisayar ters DNS adını değiştirdi. 69.63.184.145 adresindeki ana bilgisayar ilk taramada tamamen yokken ikinci taramada ortaya çıktı.

Örnek 16.1. Ndiff metin çıktısı

```
-Nmap 4.85BETA3 at 2009-03-15 11:00
+Nmap 4.85BETA4 at 2009-03-18 11:00

 photos-cache-snc1.facebook.com (69.63.178.41):
 Host is up.
 Not shown: 99 filtered ports
 PORT   STATE SERVICE VERSION
-80/tcp open  http
+80/tcp open  http    lighttpd 1.5.0

-cm.out.snc1.tfbnw.net (69.63.179.25):
+mailout-snc1.facebook.com (69.63.179.25):
 Host is up.
 Not shown: 100 filtered ports

+69.63.184.145:
+Host is up.
+Not shown: 98 filtered ports
+PORT    STATE SERVICE  VERSION
+80/tcp  open  http     Apache httpd 1.3.41.fb1
+443/tcp open  ssl/http Apache httpd 1.3.41.fb1
```

Diğer programlar tarafından işlenmesi amaçlanan XML çıktısı --xml seçeneği ile seçilir. Nmap'in XML çıktısına dayanır ve farklılıkları belirtmek için birkaç ek öğe içerir. XML belgesi nmapdiff ve scandiff öğeleri ile çevrelenmiştir. Ana bilgisayar farklılıkları hostdiff etiketleri ve bağlantı noktası farklılıkları portdiff etiketleri içine alınır. Bir hostdiff veya portdiff içinde, a ve b etiketleri ana bilgisayarın veya bağlantı noktasının ilk taramadaki (a) veya ikinci taramadaki (b) durumunu gösterir.

Örnek 16.2, yukarıda Örnek 16.1'de gösterilen aynı taramaların XML farkını göstermektedir. photos-cache-snc1.facebook.com'un 80 numaralı bağlantı noktasının portdiff etiketleri içine nasıl alındığına dikkat edin. 69.63.179.25 için eski ana bilgisayar adı a etiketinde, yenisi ise b etiketinde yer almaktadır. 69.63.184.145 numaralı yeni ana bilgisayar için, hostdiff'te karşılık gelen bir a olmadan bir b vardır, bu da ilk taramada ana bilgisayar için hiçbir bilgi olmadığını gösterir.

Örnek 16.2. Ndiff XML çıktısı

```
<?xml version="1.0" encoding="UTF-8"?>
<nmapdiff version="1">
  <scandiff>
    <hostdiff>
      <host>
        <status state="up"/>
        <address addr="69.63.178.41" addrtype="ipv4"/>
        <hostnames>
          <hostname name="photos-cache-snc1.facebook.com"/>
        </hostnames>
        <ports>
          <extraports count="99" state="filtered"/>
          <portdiff>
            <port portid="80" protocol="tcp">
              <state state="open"/>
              <a>
                <service name="http"/>
              </a>
              <b>
                <service name="http" product="lighttpd" version="1.5.0"/>
              </b>
            </port>
          </portdiff>
        </ports>
      </host>
    </hostdiff>
    <hostdiff>
      <host>
        <status state="up"/>
        <address addr="69.63.179.25" addrtype="ipv4"/>
        <hostnames>
          <a>
            <hostname name="cm.out.snc1.tfbnw.net"/>
          </a>
          <b>
            <hostname name="mailout-snc1.facebook.com"/>
          </b>
        </hostnames>
        <ports>
          <extraports count="100" state="filtered"/>
        </ports>
      </host>
    </hostdiff>
    <hostdiff>
      <b>
        <host>
          <status state="up"/>
          <address addr="69.63.184.145" addrtype="ipv4"/>
          <ports>
            <extraports count="98" state="filtered"/>
            <port portid="80" protocol="tcp">
              <state state="open"/>
              <service name="http" product="Apache httpd"
                       version="1.3.41.fb1"/>
            </port>
            <port portid="443" protocol="tcp">
              <state state="open"/>
              <service name="http" product="Apache httpd" tunnel="ssl"
                       version="1.3.41.fb1"/>
            </port>
          </ports>
        </host>
      </b>
    </hostdiff>
  </scandiff>
</nmapdiff>
```

Periodic Diffs (Periyodik Farklar)

Nmap, Ndiff, cron ve bir kabuk betiği kullanarak, bir ağı günlük olarak taramak ve ağın durumu ve önceki taramadan bu yana olan değişiklikler hakkında e-posta raporları almak mümkündür. Örnek 16.3'te bunu birbirine bağlayan komut dosyası gösterilmektedir.

Örnek 16.3. Ndiff ve cron ile bir ağı periyodik olarak tarama

```
#!/bin/sh
TARGETS="<targets>"
OPTIONS="-v -T4 -F -sV"
date=`date +%F`
cd /root/scans
nmap $OPTIONS $TARGETS -oA scan-$date > /dev/null
if [ -e scan-prev.xml ]; then
        ndiff scan-prev.xml scan-$date.xml > diff-$date
        echo "*** NDIFF RESULTS ***"
        cat diff-$date
        echo
fi
echo "*** NMAP RESULTS ***"
cat scan-$date.nmap
ln -sf scan-$date.xml scan-prev.xml
```

Betik /root/scan-ndiff.sh olarak kaydedilmişse, root'un crontab'ına aşağıdaki satırı ekleyin:

```
0 12 * * * /root/scan-ndiff.sh
```

Exit Code (Çıkış Kodu)

Çıkış kodu, taramaların eşit olup olmadığını gösterir.

- 0, taramaların Ndiff'in bildiği tüm yönlerden aynı olduğu anlamına gelir.
- 1 taramaların farklı olduğu anlamına gelir.
- 2, bir dosyanın açılamaması gibi bir çalışma zamanı hatasını belirtir.

Bugs (Hatalar)

Hataları dev@nmap.org adresindeki nmap-dev posta listesine bildirin.

History (Geçmiş)

Ndiff, 2008 Google Summer of Code sırasında Michael Pattrick tarafından bir proje olarak başlatılmıştır. Michael programı tasarladı ve çıktı formatlarının tartışılmasına öncülük etti. Programın Perl ve C++ versiyonlarını yazdı, ancak Windows (ve Zenmap) uyumluluğu için programın Python'da yeniden yazılmasına karar verilmesinden kısa bir süre sonra yaz sona erdi. Bu Python sürümü David Fifield tarafından yazılmıştır. James Levine 2000 yılında benzer işlevselliğe sahip Ndiff adlı bir Perl betiği yayınladı.

Authors (Yazarlar)

David Fifield david@bamsoftware.com

Michael Pattrick mpattrick@rhinovirus.org

Web site (Web sitesi)

https://nmap.org/ndiff/

Chapter 17. Ncat Reference Guide (Bölüm 17. Ncat Referans Kılavuzu)

İçindekiler

- Ncat Copyright and Licensing (Ncat Telif Hakkı ve Lisanslama)
- Creative Commons License for this Ncat Guide (Bu Ncat Kılavuzu için Creative Commons Lisansı)
- Source Code Availability and Community Contributions (Kaynak Kod Kullanılabilirliği ve Topluluk Katkıları)
- No Warranty (Garanti Yok)
- Inappropriate Usage (Uygunsuz Kullanım)
- Third-Party Software (Üçüncü Taraf Yazılım)

Description (Açıklama)

ncat - Soketleri birleştirir ve yeniden yönlendirir

Synopsis

`ncat` [*<OPTIONS>* ...] [*<hostname>*] [*<port>*]

Ncat, komut satırından ağlar arasında veri okuyan ve yazan özelliklerle dolu bir ağ yardımcı programıdır. Ncat, Nmap Projesi için yazılmıştır ve şu anda parçalanmış Netcat enkarnasyon ailesinin doruk noktasıdır. Diğer uygulamalara ve kullanıcılara anında ağ bağlantısı sağlamak için güvenilir bir arka uç aracı olarak tasarlanmıştır. Ncat sadece IPv4 ve IPv6 ile çalışmakla kalmaz, aynı zamanda kullanıcıya neredeyse sınırsız sayıda potansiyel kullanım sağlar.

Ncat'in çok sayıda özelliği arasında Ncat'leri birbirine zincirleme yeteneği; TCP, UDP ve SCTP portlarının diğer sitelere yönlendirilmesi; SSL desteği; ve SOCKS4, SOCKS5 veya HTTP proxy'leri aracılığıyla proxy bağlantıları (isteğe bağlı proxy kimlik doğrulaması ile birlikte) bulunmaktadır. Bazı genel ilkeler çoğu uygulama için geçerlidir ve böylece normalde asla desteklemeyecek yazılımlara anında ağ desteği ekleme olanağı sağlar.

Options Summary (Seçenekler Özet)

```
Ncat 7.93SVN ( https://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
  -4                         Use IPv4 only
  -6                         Use IPv6 only
  -U, --unixsock             Use Unix domain sockets only
      --vsock                Use vsock sockets only
  -C, --crlf                 Use CRLF for EOL sequence
  -c, --sh-exec <command>    Executes the given command via /bin/sh
  -e, --exec <command>       Executes the given command
      --lua-exec <filename>  Executes the given Lua script
  -g hop1[,hop2,...]         Loose source routing hop points (8 max)
  -G <n>                     Loose source routing hop pointer (4, 8, 12, ...)
  -m, --max-conns <n>        Maximum <n> simultaneous connections
  -h, --help                 Display this help screen
  -d, --delay <time>         Wait between read/writes
  -o, --output <filename>    Dump session data to a file
  -x, --hex-dump <filename>  Dump session data as hex to a file
  -i, --idle-timeout <time>  Idle read/write timeout
  -p, --source-port port     Specify source port to use
  -s, --source addr          Specify source address to use (doesn't affect -l)
  -l, --listen               Bind and listen for incoming connections
  -k, --keep-open            Accept multiple connections in listen mode
  -n, --nodns                Do not resolve hostnames via DNS
  -t, --telnet               Answer Telnet negotiations
  -u, --udp                  Use UDP instead of default TCP
      --sctp                 Use SCTP instead of default TCP
  -v, --verbose              Set verbosity level (can be used several times)
  -w, --wait <time>          Connect timeout
  -z                         Zero-I/O mode, report connection status only
      --append-output        Append rather than clobber specified output files
      --send-only            Only send data, ignoring received; quit on EOF
      --recv-only            Only receive data, never send anything
      --no-shutdown          Continue half-duplex when receiving EOF on stdin
      --allow                Allow only given hosts to connect to Ncat
      --allowfile            A file of hosts allowed to connect to Ncat
      --deny                 Deny given hosts from connecting to Ncat
      --denyfile             A file of hosts denied from connecting to Ncat
      --broker               Enable Ncat's connection brokering mode
      --chat                 Start a simple Ncat chat server
      --proxy <addr[:port]>  Specify address of host to proxy through
      --proxy-type <type>    Specify proxy type ("http", "socks4", "socks5")
      --proxy-auth <auth>    Authenticate with HTTP or SOCKS proxy server
      --proxy-dns <type>     Specify where to resolve proxy destination
      --ssl                  Connect or listen with SSL
      --ssl-cert             Specify SSL certificate file (PEM) for listening
      --ssl-key              Specify SSL private key (PEM) for listening
      --ssl-verify           Verify trust and domain name of certificates
      --ssl-trustfile        PEM file containing trusted SSL certificates
      --ssl-ciphers          Cipherlist containing SSL ciphers to use
      --ssl-servername       Request distinct server name (SNI)
      --ssl-alpn             ALPN protocol list to use
      --version              Display Ncat's version information and exit

See the ncat(1) manpage for full options, descriptions and usage examples
```

Connect Mode and Listen Mode (Bağlantı Modu ve Dinleme Modu)

Ncat iki ana moddan birinde çalışır: bağlanma modu ve dinleme modu. HTTP proxy sunucusu gibi diğer modlar, bu ikisinin özel durumları olarak hareket eder.

Bağlan modunda, Ncat bir istemci olarak çalışır. Dinleme modunda ise bir sunucudur.

Bağlantı modunda, <hostname> ve <port> argümanları neye bağlanılacağını belirtir. <hostname> zorunludur ve bir ana bilgisayar adı veya IP adresi olabilir. <port> verilirse, ondalık bir bağlantı noktası numarası olmalıdır. Atlanırsa, varsayılan değer 31337'dir.

Dinleme modunda, <hostname> ve <port> sunucunun bağlanacağı adresi kontrol eder. Dinleme modunda her iki bağımsız değişken de isteğe bağlıdır. <hostname> atlanırsa, varsayılan olarak IPv4 ve IPv6 üzerinden mevcut tüm adresleri dinler. <port> atlanırsa, varsayılan değer 31337 olur.

Protocol Options (Protokol Seçenekleri)

`-4` (IPv4 only) ⇒ Yalnızca IPv4 kullanımını zorlayın.

`-6` (IPv6 only) ⇒ Yalnızca IPv6 kullanımını zorlayın.

`-U`, `--unixsock` (Use Unix domain sockets) ⇒ Ağ soketleri yerine Unix etki alanı soketlerini kullanın. Bu seçenek akış soketleri için tek başına veya datagram soketleri için --udp ile birlikte kullanılabilir. U modunun açıklaması "Unix Etki Alanı Soketleri" adlı bölümde yer almaktadır.

`-u`, `--udp` (Use UDP) ⇒ Bağlantı için UDP kullanın (varsayılan TCP'dir).

`--sctp` (Use SCTP) ⇒ Bağlantı için SCTP kullanın (varsayılan TCP'dir). SCTP desteği TCP uyumlu modda uygulanır.

`--vsock` (Use AF_VSOCK sockets) ⇒ Varsayılan TCP soketleri yerine AF_VSOCK soketlerini kullanın (yalnızca Linux). Bu seçenek akış soketleri için tek başına veya datagram soketleri için --udp ile birlikte kullanılabilir. vsock modunun açıklaması "AF_VSOCK Soketleri" adlı bölümde yer almaktadır.

Connect Mode Options (Bağlantı Modu Seçenekleri)

`-g <hop1> [, <hop2> ,...]` (Loose source routing) ⇒ IPv4 gevşek kaynak yönlendirmesi için atlamaları ayarlar. Virgülle ayrılmış atlama listesiyle bir kez -g kullanabilir, listeyi oluşturmak için tek bir atlamayla birden çok kez -g kullanabilir veya ikisini birleştirebilirsiniz. Atlamalar IP adresleri veya ana bilgisayar adları olarak verilebilir.

`-G <ptr>` (Set source routing pointer) ⇒ g ile kullanılmak üzere IPv4 kaynak rota "işaretçisini" ayarlar. Bağımsız değişken 4'ün katı olmalı ve 28'den fazla olmamalıdır. Tüm işletim sistemleri bu işaretçinin dörtten başka bir değere ayarlanmasını desteklemez.

`-p <port>`, `--source-port <port>` (Specify source port) ⇒ Ncat'in bağlanacağı port numarasını ayarlayın.

`-s <host>`, `--source <host>` (Specify source address) ⇒ Ncat'in bağlanacağı adresi ayarlayın.

Listen Mode Options (Dinleme Modu Seçenekleri)

Dinleyen Ncat işlemine bağlanabilecek ana bilgisayarları sınırlama hakkında bilgi için "Erişim Kontrol Seçenekleri" adlı bölüme bakın.

`-l`, `--listen` (Listen for connections) ⇒ Uzaktaki bir makineye bağlanmak yerine bağlantıları dinleyin

`-m <numconns>`, `--max-conns <numconns>` (Specify maximum number of connections) ⇒ Bir Ncat örneği tarafından kabul edilen maksimum eşzamanlı bağlantı sayısı. 100 varsayılandır (Windows'ta 60).

`-k`, `--keep-open` (Accept multiple connections) ⇒ Normalde bir dinleme sunucusu yalnızca bir bağlantı kabul eder ve bağlantı kapandığında çıkar. Bu seçenek aynı anda birden fazla bağlantıyı kabul etmesini ve hepsi kapandıktan sonra daha fazla bağlantı beklemesini sağlar. Bu seçenek --listen ile birlikte kullanılmalıdır. Bu modda Ncat'in ağ girdisinin ne zaman bittiğini bilmesinin bir yolu yoktur, bu nedenle kesintiye uğrayana kadar çalışmaya devam edecektir. Bu aynı zamanda çıktı akışını asla kapatmayacağı anlamına gelir, bu nedenle Ncat'ten okuyan ve dosya sonunu arayan herhangi bir program da askıda kalacaktır.

`--broker` (Connection brokering) ⇒ Birden fazla tarafın merkezi bir Ncat sunucusuna bağlanmasına ve birbirleriyle iletişim kurmasına izin verin. Ncat, bir NAT arkasında olan veya başka bir şekilde doğrudan bağlanamayan sistemler arasındaki iletişime aracılık edebilir. Bu seçenek --listen ile birlikte kullanılır, bu da --listen bağlantı noktasının aracı modunun etkin olmasına neden olur.

`--chat` (Ad-hoc "chat server") ⇒ Sohbet seçeneği, birkaç kullanıcı arasında metin alışverişi için tasarlanan sohbet modunu etkinleştirir. Sohbet modunda, bağlantı aracılığı açıktır. Ncat alınan her mesajı diğer bağlantılara iletmeden önce bir ID ile ön ekler. Kimlik, bağlı her istemci için benzersizdir. Bu, kimin ne gönderdiğini ayırt etmeye yardımcı olur. Ayrıca, kontrol karakterleri gibi yazdırılmayan karakterlerin terminale zarar vermesini önlemek için kaçış yapılır.

SSL Options (SSL Seçenekleri)

`--ssl` (Use SSL) ⇒ Bağlan modunda, bu seçenek bağlantıyı güvenli bir şekilde şifrelemek için bir SSL sunucusuyla şeffaf bir şekilde SSL oturumu görüşmesi yapar. Bu özellikle SSL özellikli HTTP sunucuları vb. ile konuşmak için kullanışlıdır.

- Sunucu modunda, bu seçenek düz tünelsiz trafik yerine gelen SSL bağlantılarını dinler.
- UDP modunda, bu seçenek Datagram TLS'yi (DTLS) etkinleştirir.

`--ssl-verify` (Verify server certificates) ⇒ İstemci modunda --ssl-verify, sunucu sertifikasının doğrulanmasını gerektirmesi dışında --ssl gibidir. Ncat, ca-bundle.crt dosyasında varsayılan bir dizi güvenilir sertifika ile birlikte gelir. Bazı işletim sistemleri varsayılan bir güvenilen sertifikalar listesi sağlar; varsa bunlar da kullanılacaktır. Özel bir liste vermek için --ssl-trustfile kullanın. Doğrulama hataları hakkında ayrıntı almak için -v öğesini bir veya daha fazla kez kullanın.

- Ncat iptal edilmiş sertifikaları kontrol etmez.
- Bu seçeneğin sunucu modunda hiçbir etkisi yoktur.

`--ssl-cert` *`<certfile.pem>`* (Specify SSL certificate) ⇒ Bu seçenek, sunucunun (dinleme kipinde) veya istemcinin (bağlanma kipinde) kimliğini doğrulamak için kullanılan

PEM kodlu sertifika dosyalarının konumunu verir. Bunu --ssl-key ile birlikte kullanın.

`--ssl-key` `<keyfile.pem>` (Specify SSL private key) ⇒ Bu seçenek, --ssl-cert ile adlandırılan sertifika ile birlikte gelen PEM kodlu özel anahtar dosyasının konumunu verir.

`--ssl-trustfile` `<cert.pem>` (List trusted certificates) ⇒ Bu seçenek, sertifika doğrulama amacıyla güvenilen sertifikaların bir listesini ayarlar. --ssl-verify ile birlikte kullanılmadığı sürece hiçbir etkisi yoktur. Bu seçeneğin argümanı, güvenilen sertifikaları içeren bir PEM dosyasının adıdır. Tipik olarak, dosya sertifika yetkililerinin sertifikalarını içerecektir, ancak doğrudan sunucu sertifikalarını da içerebilir. Bu seçenek kullanıldığında, Ncat varsayılan sertifikalarını kullanmaz.

`--ssl-ciphers` `<cipherlist>` (Specify SSL ciphersuites) ⇒ Bu seçenek, Ncat'in sunuculara bağlanırken veya istemcilerden SSL bağlantılarını kabul ederken kullanacağı şifrelerin listesini ayarlar. Sözdizimi OpenSSL ciphers(1) man sayfasında açıklanmıştır ve varsayılan olarak ALL:!aNULL:!eNULL:!LOW:!EXP:!RC4:!MD5:@STRENGTH

`--ssl-servername` `<name>` (Request distinct server name) ⇒ İstemci modunda bu seçenek, sunucuya Ncat'in iletişim kurduğu mantıksal sunucunun adını söyleyen TLS SNI (Sunucu Adı Göstergesi) uzantısını ayarlar. Bu, hedef sunucu tek bir temel ağ adresinde birden fazla sanal sunucu barındırdığında önemlidir. Bu seçenek sağlanmazsa, TLS SNI uzantısı hedef sunucu ana bilgisayar adıyla doldurulur.

`--ssl-alpn` `<ALPN list>` (Specify ALPN protocol list) ⇒ Bu seçenek, Uygulama Katmanı Protokol Anlaşması (ALPN) TLS uzantısı aracılığıyla gönderilecek protokollerin virgülle ayrılmış bir listesini belirtmenize olanak tanır. OpenSSL'in tüm sürümleri tarafından desteklenmez.

Proxy Options (Proxy Seçenekleri)

`--proxy` `<host>` `[:` `<port>` `]` (Specify proxy address) ⇒ proxy-type ile belirtilen protokolü kullanarak <host>:<port> üzerinden proxy'leme talep eder. Herhangi bir bağlantı noktası belirtilmezse, proxy protokolünün iyi bilinen bağlantı noktası kullanılır (SOCKS için 1080 ve HTTP için 3128). Ana bilgisayar adı yerine IP adresi

kullanarak bir IPv6 HTTP proxy sunucusu belirtirken, bağlantı noktasını IPv6 adresinden ayırmak için köşeli parantez gösterimi (örneğin [2001:db8::1]:8080) kullanılmalıdır. Proxy kimlik doğrulaması gerektiriyorsa --proxy-auth kullanın.

`--proxy-type` `<proto>` (Specify proxy protocol) ⇒ Bağlan modunda, bu seçenek <proto> protokolünün --proxy ile belirtilen proxy ana bilgisayarı üzerinden bağlanmasını ister. Dinle modunda, bu seçenek Ncat'in belirtilen protokolü kullanarak bir proxy sunucusu gibi davranmasını sağlar.

Bağlantı modunda şu anda mevcut olan protokoller http (CONNECT), socks4 (SOCKSv4) ve socks5'tir (SOCKSv5). Şu anda desteklenen tek sunucu http'dir. Bu seçenek kullanılmazsa, varsayılan protokol http'dir.

`--proxy-auth` `<user>` `[:` `<pass>` `]` (Specify proxy credentials) ⇒ Bağlan modunda, proxy sunucusuna bağlanmak için kullanılacak kimlik bilgilerini verir. Dinleme modunda, bağlanan istemcilerden istenecek kimlik bilgilerini verir. proxy-type http veya --proxy-type socks5 ile kullanım için, form kullanıcı adı:şifre olmalıdır. proxy-type socks4 için sadece kullanıcı adı olmalıdır.

Bu kimlik bilgileri alternatif olarak NCAT_PROXY_AUTH ortam değişkeni ayarlanarak Ncat'e aktarılabilir, bu da kimlik bilgilerinin işlem günlüklerinde yakalanma riskini azaltır. (--proxy-auth seçeneği önceliklidir.)

`--proxy-dns` `<type>` (Specify where to resolve proxy destination) ⇒ Bağlantı modunda, proxy hedef ana bilgisayar adlarının uzak proxy sunucusu tarafından mı yoksa yerel olarak Ncat'in kendisi tarafından mı çözümleneceği üzerinde kontrol sağlar. <type> için olası değerler şunlardır:

- local - Ana bilgisayar adları Ncat ana bilgisayarında yerel olarak çözümlenir. Ana bilgisayar adı çözümlenemezse Ncat hata ile çıkar.
- remote - Ana bilgisayar adları doğrudan uzak proxy sunucusuna aktarılır. Bu varsayılan davranıştır.
- her ikisi de - Ana bilgisayar adı çözümlemesi ilk olarak Ncat ana bilgisayarında denenir. Çözümlenemeyen ana bilgisayar adları uzak proxy sunucusuna aktarılır.
- none - Ana bilgisayar adı çözümlemesi tamamen devre dışı bırakılır. Proxy hedefi olarak yalnızca gerçek bir IPv4 veya IPv6 adresi kullanılabilir.

- Yerel ana bilgisayar adı çözümlemesi, IPv6 ile uyumsuz olan SOCKS4 hariç, genellikle -4 veya -6 seçenekleriyle belirtilen IP sürümüne uyar.

Command Execution Options (Komut Yürütme Seçenekleri)

`-e` `<command>`, `--exec` `<command>` (Execute command) ⇒ Bir bağlantı kurulduktan sonra belirtilen komutu çalıştırır. Komut tam bir yol adı olarak belirtilmelidir. Uzak istemciden gelen tüm girdiler uygulamaya gönderilecek ve yanıtlar soket üzerinden uzak istemciye geri gönderilecek, böylece komut satırı uygulamanız bir soket üzerinden etkileşimli hale gelecektir. Keep-open ile birlikte Ncat, inetd gibi belirttiğiniz port/uygulamaya birden fazla eşzamanlı bağlantıyı idare edecektir. Ncat yalnızca -m seçeneği tarafından kontrol edilen maksimum, tanımlanabilir, eşzamanlı bağlantı sayısını kabul edecektir. Varsayılan olarak bu sayı 100 olarak ayarlanmıştır (Windows'ta 60).

`-c` `<command>`, `--sh-exec` `<command>` (Execute command via sh) ⇒ e ile aynıdır, ancak komutu /bin/sh üzerinden çalıştırmaya çalışır. Bu, komut için tam yolu belirtmek zorunda olmadığınız ve ortam değişkenleri gibi kabuk olanaklarının kullanılabileceği anlamına gelir.

`--lua-exec` `<file>` (Execute a .lua script) ⇒ Bir bağlantı kurulduktan sonra yerleşik bir yorumlayıcı kullanarak belirtilen dosyayı bir Lua betiği olarak çalıştırır. Betiğin hem standart girişi hem de standart çıkışı bağlantı veri akışlarına yönlendirilir.

- Tüm yürütme seçenekleri çocuğun ortamına aşağıdaki değişkenleri ekler:

`NCAT_REMOTE_ADDR`, `NCAT_REMOTE_PORT` ⇒ Uzak ana bilgisayarın IP adresi ve bağlantı noktası numarası. Bağlan modunda, hedefin adresidir; dinle modunda, istemcinin adresidir.

`NCAT_LOCAL_ADDR`, `NCAT_LOCAL_PORT` ⇒ Bağlantının yerel ucunun IP adresi ve bağlantı noktası numarası.

`NCAT_PROTO` ⇒ Kullanılan protokol: TCP, UDP ve SCTP'den biri.

Access Control Options (Erişim Kontrol Seçenekleri)

`--allow <host> [, <host> ,...]` (Allow connections) ⇒ Belirtilen ana bilgisayar listesi, Ncat işlemine bağlanmasına izin verilen tek ana bilgisayarlar olacaktır. Diğer tüm bağlantı girişimlerinin bağlantısı kesilecektir. İzin ver ve reddet arasında bir çelişki olması durumunda, --izin ver önceliklidir. Ana bilgisayar özellikleri Nmap tarafından kullanılan sözdiziminin aynısını takip eder.

`--allowfile <file>` (Allow connections from file) ⇒ Bu, --allow ile aynı işlevselliğe sahiptir, ancak izin verilen ana bilgisayarlar doğrudan komut satırında değil, yeni satırla sınırlandırılmış bir izin dosyasında sağlanır.

`--deny <host> [, <host> ,...]` (Deny connections) ⇒ Ncat'e, dinleyen Ncat sürecine bağlanmasına izin verilmeyecek ana bilgisayarların bir listesini verin. Belirtilen ana bilgisayarlar bağlanmaya çalışırlarsa oturumları sessizce sonlandırılır. izin ver ve --deny arasında bir çakışma olması durumunda, --izin ver önceliklidir. Ana bilgisayar özellikleri Nmap tarafından kullanılan sözdiziminin aynısını takip eder.

`--denyfile <file>` (Deny connections from file) ⇒ Bu, --deny ile aynı işlevdir, ancak hariç tutulan ana bilgisayarlar doğrudan komut satırında değil, yeni satırla sınırlandırılmış bir deny dosyasında sağlanır.

Timing Options (Zamanlama Seçenekleri)

Bu seçenekler bir zaman parametresi kabul eder. Bu varsayılan olarak saniye cinsinden belirtilir, ancak milisaniye, saniye, dakika veya saat belirtmek için değere ms, s, m veya h ekleyebilirsiniz.

`-d <time>`, `--delay <time>` (Specify line delay) ⇒ Gönderilen hatlar için gecikme aralığını ayarlayın. Bu, Ncat'in belirtilen süre içinde göndereceği satır sayısını etkili bir şekilde sınırlar. Bu, düşük bant genişliğine sahip siteler için yararlı olabilir veya can sıkıcı iptables --limit seçenekleriyle başa çıkmak gibi başka kullanımları da olabilir.

`-i <time>`, `--idle-timeout <time>` (Specify idle timeout) ⇒ Boşta kalan bağlantılar için sabit bir zaman aşımı ayarlayın. Boşta kalma zaman aşımına ulaşılırsa, bağlantı sonlandırılır.

`-w <time>`, `--wait <time>` (Specify connect timeout) ⇒ Bağlantı denemeleri için sabit bir zaman aşımı ayarlayın.

Output Options (Çıktı Seçenekleri)

`-o <file>`, `--output <file>` (Save session data) ⇒ Oturum verilerini bir dosyaya dökme

`-x <file>`, `--hex-dump <file>` (Save session data in hex) ⇒ Oturum verilerini hex olarak bir dosyaya döker.

`--append-output` (Append output) ⇒ Ncat'i -o ve/veya -x ile birlikte --append-ouput ile çalıştırdığınızda, belirtilen çıktı dosyalarını kesmek yerine sonuç çıktısını ekleyecektir.

`-v`, `--verbose` (Be verbose) ⇒ Ncat'i -v ile çalıştırdığınızda ayrıntılı olacak ve her türlü yararlı bağlantı tabanlı bilgiyi görüntüleyecektir. Daha fazla ayrıntı için birden fazla kez (-vv, -vvv...) kullanın.

Misc Options (Çeşitli Seçenekler)

`-C`, `--crlf` (Use CRLF as EOL) ⇒ Bu seçenek Ncat'e standart girdiden girdi alırken LF satır sonlarını CRLF'ye dönüştürmesini söyler. Bu, satır sonu için CRLF kullanan birçok yaygın düz metin protokolünden birinde bazı katı sunucularla doğrudan bir terminalden konuşmak için kullanışlıdır.

`-h`, `--help` (Help screen) ⇒ Genel seçenekleri ve parametreleri içeren kısa bir yardım ekranı görüntüler ve ardından çıkar.

`--recv-only` (Only receive data) ⇒ Bu seçenek geçilirse, Ncat yalnızca veri alacak ve herhangi bir şey göndermeye çalışmayacaktır.

`--send-only` (Only send data) ⇒ Bu seçenek geçilirse, Ncat yalnızca veri gönderir ve alınan her şeyi yok sayar. Bu seçenek ayrıca Ncat'in ağ bağlantısını kapatmasına ve standart girdiden EOF alındıktan sonra sonlandırılmasına neden olur.

`--no-shutdown` (Do not shutdown into half-duplex mode) ⇒ Bu seçenek geçilirse, Ncat stdin'de EOF gördükten sonra bir soket üzerinde kapatma çağrısı yapmayacaktır. Bu, '-d' seçeneği ile çalıştırıldığında bu davranışı sergileyen OpenBSD netcat ile geriye dönük uyumluluk için sağlanmıştır.

`-n`, `--nodns` (Do not resolve hostnames) ⇒ Hedef, kaynak adres, kaynak yönlendirme atlamaları ve proxy gibi tüm Ncat seçeneklerinde ana bilgisayar adı çözümlemesini tamamen devre dışı bırakın. Tüm adresler sayısal olarak belirtilmelidir. (Proxy hedeflerinin çözünürlüğünün --proxy-dns seçeneği ile ayrı olarak kontrol edildiğini unutmayın).

`-t`, `--telnet` (Answer Telnet negotiations) ⇒ DO/DONT WILL/WONT Telnet görüşmelerini ele alır. Bu, Telnet oturumlarını Ncat ile komut dosyası haline getirmeyi mümkün kılar.

`--version` (Display version) ⇒ Ncat sürüm numarasını görüntüler ve çıkar.

Unix Domain Sockets (Unix Etki Alanı Soketleri)

U seçeneği (--unixsock ile aynı) Ncat'in ağ soketleri yerine Unix etki alanı soketlerini kullanmasına neden olur. Unix etki alanı soketleri dosya sisteminde bir girdi olarak bulunur. Bağlanmak veya dinlemek için bir soket adı vermelisiniz. Örneğin, bir bağlantı yapmak için,

ncat -U ~/unixsock ⇒

Bir soketi dinlemek için:

ncat -l -U ~/unixsock ⇒

Dinleme modu, mevcut değilse soketi oluşturacaktır. Program sona erdikten sonra soket var olmaya devam edecektir.

Hem akış hem de datagram etki alanı soketleri desteklenir. Akış soketleri için -U'yu tek başına kullanın veya datagram soketleri için --udp ile birleştirin. Datagram soketleri bağlanmak için bir kaynak soket gerektirir. Varsayılan olarak, rastgele bir dosya adına sahip bir kaynak soketi gerektiğinde oluşturulacak ve program sona erdiğinde silinecektir. Belirli bir ada sahip bir kaynak soketi kullanmak için --source komutunu bir yol ile birlikte kullanın.

AF_VSOCK Sockets (AF_VSOCK Soketleri)

vsock seçeneği Ncat'in ağ soketleri yerine AF_VSOCK soketlerini kullanmasına neden olur. Ana bilgisayar adı veya IP adresi yerine bir CID verilmelidir. Örneğin, ana bilgisayara bağlantı yapmak için,

ncat --vsock 2 1234

Bir soketi dinlemek için:

ncat -l --vsock 1234

Hem akış hem de datagram etki alanı soketleri desteklenir, ancak soket türünün kullanılabilirliği hipervizöre bağlıdır. Akış soketleri için --vsock'u tek başına kullanın veya datagram soketleri için --udp ile birleştirin.

Examples (Örnekler)

TCP bağlantı noktası 8080 üzerinden example.org'a bağlanın.

ncat example.org 8080

TCP bağlantı noktası 8080'deki bağlantıları dinleyin.

ncat -l 8080

Yerel makinedeki 8080 numaralı TCP bağlantı noktasını 80 numaralı bağlantı noktasındaki ana bilgisayara yönlendirin.

ncat --sh-exec "ncat example.org 80" -l 8080 --keep-open

TCP portu 8081'e bağlayın ve dünyanın serbestçe erişebilmesi için /bin/bash ekleyin.

ncat --exec "/bin/bash" -l 8081 --keep-open

TCP bağlantı noktası 8081'e bir kabuk bağlayın, yerel ağdaki ana bilgisayarlara erişimi sınırlayın ve maksimum eşzamanlı bağlantı sayısını 3 ile sınırlayın.

ncat --exec "/bin/bash" --max-conns 3 --allow 192.168.0.0/24 -l 8081 --keep-open

1080 numaralı bağlantı noktasındaki bir SOCKS4 sunucusu aracılığıyla smtphost:25'e bağlanın.

ncat --proxy socks4host --proxy-type socks4 --proxy-auth joe smtphost 25

1080 numaralı bağlantı noktasındaki bir SOCKS5 sunucusu aracılığıyla smtphost:25'e bağlanın.

ncat --proxy socks5host --proxy-type socks5 --proxy-auth joe:secret smtphost 25

localhost bağlantı noktası 8888 üzerinde bir HTTP proxy sunucusu oluşturun.

ncat -l --proxy-type http localhost 8888

TCP bağlantı noktası 9899 üzerinden ana bilgisayar2'den (istemci) ana bilgisayar1'e (sunucu) bir dosya gönderin.

HOST1$ **ncat -l 9899 > outputfile**

HOST1$ **ncat -l 9899 > outputfile**

Diğer yönde aktarım, Ncat'i bir "tek dosya" sunucusuna dönüştürür.

HOST1$ **ncat -l 9899 < inputfile**

HOST2$ **ncat HOST1 9899 > outputfile**

Exit Code (Çıkış Kodu)

Çıkış kodu, bir bağlantının yapılıp yapılmadığını ve başarıyla tamamlanıp tamamlanmadığını yansıtır. 0 hata olmadığı anlamına gelir. 1 bir tür ağ hatası olduğu anlamına gelir, örneğin "Bağlantı reddedildi" veya "Bağlantı sıfırlandı". 2, geçersiz bir seçenek veya var olmayan bir dosya gibi diğer tüm hatalar için ayrılmıştır.

Bugs (Hatalar)

Yazarları gibi Ncat de mükemmel değildir. Ancak hata raporları göndererek ve hatta yamalar yazarak daha iyi olmasına yardımcı olabilirsiniz. Ncat beklediğiniz gibi davranmazsa, önce https://nmap.org adresinden ulaşabileceğiniz en son sürüme yükseltin. Sorun devam ederse, daha önce keşfedilmiş ve ele alınmış olup olmadığını belirlemek için biraz araştırma yapın. Hata mesajını Google'da aramayı veya https://seclists.org/ adresindeki nmap-dev arşivlerine göz atmayı deneyin. Bu kılavuz sayfasının tamamını da okuyun. Bundan bir şey çıkmazsa, dev@nmap.org adresine bir hata raporu gönderin. Lütfen sorunla ilgili öğrendiğiniz her şeyi ve hangi Ncat sürümünü çalıştırdığınızı ve hangi işletim sistemi sürümünde çalıştığını ekleyin. dev@nmap.org adresine gönderilen sorun raporları ve Ncat kullanım sorularının yanıtlanma olasılığı, doğrudan Fyodor'a gönderilenlerden çok daha yüksektir.

Authors (Yazarlar)

- Chris Gibson `<chris@linuxops.net>`
- Gordon Lyon (Fyodor) `<fyodor@nmap.org>` (`http://insecure.org`)
- Kris Katterjohn `<katterjohn@gmail.com>`
- Mixter `<mixter@gmail.com>`

Orijinal Netcat *Hobbit* hobbit@avian.org tarafından yazılmıştır. Ncat, "geleneksel" Netcat'ten (veya başka bir uygulamadan) herhangi bir kod üzerine inşa edilmemiş olsa da, Ncat kesinlikle ruh ve işlevsellik açısından Netcat'e dayanmaktadır.

Legal Notices (Yasal Uyarılar)

Ncat Telif Hakkı ve Lisanslama

Bu Ncat Kılavuzu için Creative Commons Lisansı

Bu Ncat Referans Kılavuzu (C) 2005-2022 Nmap Software LLC'ye aittir. Creative Commons Attribution License'ın 3.0 sürümü altında yer almaktadır. Bu, orijinal kaynağa atıfta bulunduğunuz sürece çalışmayı istediğiniz gibi yeniden dağıtmanıza ve değiştirmenize izin verir. Alternatif olarak, bu belgeyi Ncat'in kendisi ile aynı lisans altında değerlendirmeyi seçebilirsiniz (daha önce tartışılmıştır).

Kaynak Kodunun Kullanılabilirliği ve Topluluk Katkıları

Kullanıcıların bir programı çalıştırmadan önce tam olarak ne yapacağını bilmeye hakları olduğuna inandığımız için bu yazılıma kaynak sağlanmıştır. Bu aynı zamanda yazılımı güvenlik açıklarına karşı denetlemenize de olanak tanır (şimdiye kadar hiçbiri bulunamadı).

Kaynak kodu ayrıca Nmap'i (Ncat içerir) yeni platformlara taşımanıza, hataları düzeltmenize ve yeni özellikler eklemenize olanak tanır. Ana dağıtıma dahil edilebilmesi için değişikliklerinizi dev@nmap.org adresine göndermeniz önemle tavsiye edilir. Bu değişiklikleri Fyodor'a veya Insecure.Org geliştirme posta listelerinden birine göndererek, Nmap Projesi'ne (Nmap Software LLC) kodu yeniden kullanma, değiştirme ve yeniden lisanslama için sınırsız, münhasır olmayan bir hak sunduğunuz varsayılır. Nmap her zaman açık kaynak olarak sunulacaktır, ancak bu önemlidir çünkü kodun yeniden lisanslanamaması diğer Özgür Yazılım projeleri (KDE ve NASM gibi) için yıkıcı sorunlara neden olmuştur. Ayrıca Nmap man sayfasında tartışıldığı gibi zaman zaman kodu üçüncü taraflara yeniden lisanslıyoruz. Katkılarınız için özel lisans koşulları belirtmek isterseniz, bunları gönderirken belirtmeniz yeterlidir.

Garanti Yok

Bu program yararlı olacağı umuduyla, ancak HERHANGİ BİR GARANTİ OLMAKSIZIN; hatta ZIMNİ SATILABİLİRLİK veya BELİRLİ BİR AMACA UYGUNLUK garantisi olmaksızın dağıtılmaktadır. Daha fazla ayrıntı için https://nmap.org/npsl/ adresindeki Nmap Kamu Kaynak Lisansı'na veya Nmap ile birlikte verilen LICENSE dosyasına bakın.

Uygunsuz Kullanım

Ncat asla özel ayrıcalıklarla (örn. suid root) kurulmamalıdır. Bu, sistemdeki diğer kullanıcılar (veya saldırganlar) ayrıcalık yükseltmek için kullanabileceğinden büyük bir güvenlik açığına yol açacaktır.

Üçüncü Taraf Yazılımlar

Bu ürün Apache Software Foundation tarafından geliştirilen yazılımları içerir. Libpcap taşınabilir paket yakalama kütüphanesinin değiştirilmiş bir sürümü Ncat ile birlikte dağıtılır. Ncat'in Windows sürümü bunun yerine Libpcap türevi Npcap kütüphanesini kullanmıştır. Bazı ham ağ işlevleri Dug Song tarafından yazılmış olan Libdnet ağ kütüphanesini kullanır. Değiştirilmiş bir sürümü Ncat ile birlikte dağıtılmaktadır. Ncat isteğe bağlı olarak SSL sürüm algılama desteği için OpenSSL kriptografi araç seti ile bağlantı kurabilir. Bu paragrafta açıklanan tüm üçüncü taraf yazılımlar BSD tarzı yazılım lisansları altında serbestçe yeniden dağıtılabilir.

Chapter 18. Nping Reference Guide (Bölüm 18. Nping Referans Kılavuzu)

İçindekiler

Description (Açıklama)

nping - Ağ paketi oluşturma aracı / ping yardımcı programı

`nping` [*<Options>*] { *<targets>* }

Not : Bu belge, https://nmap.org/nping adresinde bulunan en son Nping sürümünü açıklamaktadır. Lütfen bir özelliğin açıklandığı gibi çalışmadığını bildirmeden önce en son sürümü kullandığınızdan emin olun.

Nping, ağ paketi oluşturma, yanıt analizi ve yanıt süresi ölçümü için açık kaynaklı bir araçtır. Nping, kullanıcıların çok çeşitli protokollerin ağ paketlerini oluşturmalarına ve protokol başlıklarının hemen hemen her alanını ayarlamalarına olanak tanır. Nping, aktif ana bilgisayarları tespit etmek için basit bir ping yardımcı programı olarak kullanılabildiği gibi, ağ yığını stres testleri, ARP zehirlenmesi, Hizmet Reddi saldırıları, rota izleme ve diğer amaçlar için ham paket oluşturucu olarak da kullanılabilir.

Buna ek olarak, Nping "Yankı Modu" adı verilen özel bir çalışma modu sunar, bu sayede kullanıcılar oluşturulan probların geçiş sırasında nasıl değiştiğini görebilir, iletilen paketler ile diğer uçta alınan paketler arasındaki farkları ortaya çıkarabilir. Ayrıntılar için "Yankı Modu" bölümüne bakın.

Nping'in çıktısı, gönderilen ve alınan paketlerin bir listesidir. Ayrıntı düzeyi kullanılan seçeneklere bağlıdır.

Tipik bir Nping uygulaması Örnek 18.1'de gösterilmektedir. Bu örnekte kullanılan tek Nping argümanları, her bir ana bilgisayarın kaç kez hedefleneceğini belirtmek için -c, TCP Prob Modunu belirtmek için --tcp, hedef portları belirtmek için -p 80,433; ve ardından iki hedef ana bilgisayar adıdır.

Örnek 18.1. Temsili bir Nping uygulaması

```
# nping -c 1 --tcp -p 80,433 scanme.nmap.org google.com

Starting Nping ( https://nmap.org/nping )
SENT (0.0120s) TCP 96.16.226.135:50091 > 64.13.134.52:80 S ttl=64 id=52072 iplen=40  seq=1077657388 win=1480
RCVD (0.1810s) TCP 64.13.134.52:80 > 96.16.226.135:50091 SA ttl=53 id=0 iplen=44  seq=4158134847 win=5840 <mss 1460>
SENT (1.0140s) TCP 96.16.226.135:50091 > 74.125.45.100:80 S ttl=64 id=13932 iplen=40  seq=1077657388 win=1480
RCVD (1.1370s) TCP 74.125.45.100:80 > 96.16.226.135:50091 SA ttl=52 id=52913 iplen=44  seq=2650443864 win=5720 <mss 1430>
SENT (2.0140s) TCP 96.16.226.135:50091 > 64.13.134.52:433 S ttl=64 id=8373 iplen=40  seq=1077657388 win=1480
SENT (3.0140s) TCP 96.16.226.135:50091 > 74.125.45.100:433 S ttl=64 id=23624 iplen=40  seq=1077657388 win=1480

Statistics for host scanme.nmap.org (64.13.134.52):
  |  Probes Sent: 2 | Rcvd: 1 | Lost: 1  (50.00%)
  |_ Max rtt: 169.720ms | Min rtt: 169.720ms | Avg rtt: 169.720ms
Statistics for host google.com (74.125.45.100):
  |  Probes Sent: 2 | Rcvd: 1 | Lost: 1  (50.00%)
  |_ Max rtt: 122.686ms | Min rtt: 122.686ms | Avg rtt: 122.686ms
Raw packets sent: 4 (160B) | Rcvd: 2 (92B) | Lost: 2 (50.00%)
Tx time: 3.00296s | Tx bytes/s: 53.28 | Tx pkts/s: 1.33
Rx time: 3.00296s | Rx bytes/s: 30.64 | Rx pkts/s: 0.67
Nping done: 2 IP addresses pinged in 4.01 seconds
```

Nping'in en yeni sürümü https://nmap.org adresindeki Nmap ile elde edilebilir. Bu man sayfasının en yeni sürümü https://nmap.org/book/nping-man.html adresinde mevcuttur.

Options Summary (Seçenekler Özet)

Bu seçenek özeti, Nping hiçbir argüman olmadan çalıştırıldığında yazdırılır. İnsanların en yaygın seçenekleri hatırlamasına yardımcı olur, ancak bu kılavuzun geri kalanındaki ayrıntılı belgelerin yerini tutmaz. Bazı belirsiz seçenekler buraya dahil bile edilmemiştir.

```
Nping 0.7.92SVN ( https://nmap.org/nping )
Usage: nping [Probe mode] [Options] {target specification}

TARGET SPECIFICATION:
  Targets may be specified as hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.*.1-24
PROBE MODES:
  --tcp-connect                : Unprivileged TCP connect probe mode.
  --tcp                        : TCP probe mode.
  --udp                        : UDP probe mode.
  --icmp                       : ICMP probe mode.
  --arp                        : ARP/RARP probe mode.
  --tr, --traceroute           : Traceroute mode (can only be used with
                               TCP/UDP/ICMP modes).
TCP CONNECT MODE:
   -p, --dest-port <port spec>     : Set destination port(s).
   -g, --source-port <portnumber>  : Try to use a custom source port.
TCP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>     : Set destination port(s).
   --seq <seqnumber>               : Set sequence number.
   --flags <flag list>             : Set TCP flags (ACK,PSH,RST,SYN,FIN...)
   --ack <acknumber>               : Set ACK number.
   --win <size>                    : Set window size.
   --badsum                        : Use a random invalid checksum.
UDP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>     : Set destination port(s).
```

```
  --badsum                    : Use a random invalid checksum.
ICMP PROBE MODE:
  --icmp-type <type>            : ICMP type.
  --icmp-code <code>            : ICMP code.
  --icmp-id <id>              : Set identifier.
  --icmp-seq <n>              : Set sequence number.
  --icmp-redirect-addr <addr>     : Set redirect address.
  --icmp-param-pointer <pnt>      : Set parameter problem pointer.
  --icmp-advert-lifetime <time>   : Set router advertisement lifetime.
  --icmp-advert-entry <IP,pref>   : Add router advertisement entry.
  --icmp-orig-time  <timestamp>   : Set originate timestamp.
  --icmp-recv-time  <timestamp>   : Set receive timestamp.
  --icmp-trans-time <timestamp>   : Set transmit timestamp.
ARP/RARP PROBE MODE:
  --arp-type <type>           : Type: ARP, ARP-reply, RARP, RARP-reply.
  --arp-sender-mac <mac>        : Set sender MAC address.
  --arp-sender-ip  <addr>       : Set sender IP address.
  --arp-target-mac <mac>        : Set target MAC address.
  --arp-target-ip  <addr>       : Set target IP address.
IPv4 OPTIONS:
  -S, --source-ip             : Set source IP address.
  --dest-ip <addr>              : Set destination IP address (used as an
                          alternative to {target specification} ).
  --tos <tos>                 : Set type of service field (8bits).
  --id  <id>                  : Set identification field (16 bits).
  --df                        : Set Don't Fragment flag.
  --mf                        : Set More Fragments flag.
  --evil                      : Set Reserved / Evil flag.
  --ttl <hops>                : Set time to live [0-255].
  --badsum-ip                 : Use a random invalid checksum.
  --ip-options <S|R [route]|L [route]|T|U ...> : Set IP options
  --ip-options <hex string>               : Set IP options
  --mtu <size>                : Set MTU. Packets get fragmented if MTU is
                          small enough.
IPv6 OPTIONS:
  -6, --IPv6                  : Use IP version 6.
```

```
  --dest-ip                  : Set destination IP address (used as an
                             alternative to {target specification}).
  --hop-limit                : Set hop limit (same as IPv4 TTL).
  --traffic-class <class> :  : Set traffic class.
  --flow <label>             : Set flow label.
ETHERNET OPTIONS:
  --dest-mac <mac>           : Set destination mac address. (Disables
                             ARP resolution)
  --source-mac <mac>         : Set source MAC address.
  --ether-type <type>        : Set EtherType value.
PAYLOAD OPTIONS:
  --data <hex string>        : Include a custom payload.
  --data-string <text>       : Include a custom ASCII text.
  --data-length <len>        : Include len random bytes as payload.
ECHO CLIENT/SERVER:
  --echo-client <passphrase>   : Run Nping in client mode.
  --echo-server <passphrase>   : Run Nping in server mode.
  --echo-port <port>         : Use custom <port> to listen or connect.
  --no-crypto                : Disable encryption and authentication.
  --once                     : Stop the server after one connection.
  --safe-payloads            : Erase application data in echoed packets.
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m, 0.25h).
  --delay <time>             : Adjust delay between probes.
  --rate  <rate>             : Send num packets per second.
MISC:
  -h, --help                 : Display help information.
  -V, --version              : Display current version number.
  -c, --count <n>            : Stop after <n> rounds.
  -e, --interface <name>     : Use supplied network interface.
  -H, --hide-sent            : Do not display sent packets.
  -N, --no-capture           : Do not try to capture replies.
  --privileged               : Assume user is fully privileged.
  --unprivileged             : Assume user lacks raw socket privileges.
  --send-eth                 : Send packets at the raw Ethernet layer.
```

```
  --send-ip                   : Send packets using raw IP sockets.
  --bpf-filter <filter spec>      : Specify custom BPF filter.
OUTPUT:
  -v                        : Increment verbosity level by one.
  -v[level]                   : Set verbosity level. E.g: -v4
  -d                        : Increment debugging level by one.
  -d[level]                   : Set debugging level. E.g: -d3
  -q                        : Decrease verbosity level by one.
  -q[N]                     : Decrease verbosity level N times
  --quiet                     : Set verbosity and debug level to minimum.
  --debug                     : Set verbosity and debug to the max level.
EXAMPLES:
  nping scanme.nmap.org
  nping --tcp -p 80 --flags rst --ttl 2 192.168.1.1
  nping --icmp --icmp-type time --delay 500ms 192.168.254.254
  nping --echo-server "public" -e wlan0 -vvv
  nping --echo-client "public" echo.nmap.org --tcp -p1-1024 --flags ack

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAM
PLES
```

Target Specification (Hedef Spesifikasyonu)

Nping komut satırında bir seçenek veya seçenek argümanı olmayan her şey bir hedef ana bilgisayar belirtimi olarak değerlendirilir. Nping, hedef belirtimleri için Nmap ile aynı sözdizimini kullanır. En basit durum IP adresi veya ana bilgisayar adı ile verilen tek bir hedeftir.

Nping CIDR tarzı adreslemeyi destekler. Bir IPv4 adresine veya ana bilgisayar adına /<numbits> ekleyebilirsiniz ve Nping, ilk <numbits>'in verilen referans IP veya ana bilgisayar adıyla aynı olduğu her IP adresine prob gönderecektir. Örneğin, 192.168.10.0/24, 192.168.10.0 (binary: 11000000 10101000 00001010 00000000) ile 192.168.10.255 (binary: 11000000 10101000 00001010 11111111) arasındaki 256 ana bilgisayara prob gönderecektir. 192.168.10.40/24 tam olarak

aynı hedeflere ping atacaktır. Scanme.nmap.org ana bilgisayarının 64.13.134.52 IP adresinde olduğu düşünüldüğünde, scanme.nmap.org/16 belirtimi 64.13.0.0 ile 64.13.255.255 arasındaki 65.536 IP adresine sondalar gönderecektir. İzin verilen en küçük değer, tüm İnternet'i hedefleyen /0'dır. En büyük değer /32'dir ve tüm adres bitleri sabit olduğu için yalnızca adlandırılmış ana bilgisayarı veya IP adresini hedefler.

CIDR notasyonu kısadır ancak her zaman yeterince esnek değildir. Örneğin, 192.168.0.0/16 adresine prob göndermek isteyebilirsiniz ancak .0 veya .255 ile biten IP'leri atlayabilirsiniz çünkü bunlar alt ağ ve yayın adresleri olarak kullanılabilir. Nping bunu oktet aralığı adresleme yoluyla destekler. Normal bir IP adresi belirtmek yerine, her oktet için virgülle ayrılmış bir sayı veya aralık listesi belirtebilirsiniz. Örneğin, 192.168.0-255.1-254, aralıktaki .0 veya .255 ile biten tüm adresleri atlayacak ve 192.168.3-5,7.1, 192.168.3.1, 192.168.4.1, 192.168.5.1 ve 192.168.7.1 adreslerini hedefleyecektir. Bir aralığın her iki tarafı da atlanabilir; varsayılan değerler solda 0 ve sağda 255'tir. Tek başına - kullanmak 0-255 ile aynıdır, ancak hedef belirtiminin bir komut satırı seçeneği gibi görünmemesi için ilk sekizlide 0- kullanmayı unutmayın. Aralıkların son oktetlerle sınırlı olması gerekmez: 0-.-.13.37 belirteci, Internet'te .13.37 ile biten tüm IP adreslerine sondalar gönderecektir. Bu tür geniş örnekleme İnternet anketleri ve araştırmaları için yararlı olabilir.

IPv6 adresleri yalnızca tam nitelikli IPv6 adresleri veya ana bilgisayar adları ile belirtilebilir. CIDR ve oktet aralıkları IPv6 için desteklenmez çünkü nadiren kullanışlıdırlar.

Nping, komut satırında birden fazla ana bilgisayar belirtimini kabul eder ve bunların aynı türde olması gerekmez. nping scanme.nmap.org 192.168.0.0/8 10.0.0,1,3-7.- komutu beklediğiniz şeyi yapar.

Option Specification (Seçenek Spesifikasyonu)

Nping çok esnek olacak ve çok çeşitli ihtiyaçlara uyacak şekilde tasarlanmıştır. Çoğu komut satırı aracında olduğu gibi, davranışı komut satırı seçenekleri kullanılarak ayarlanabilir. Bu genel ilkeler, aksi belirtilmedikçe seçenek argümanları için geçerlidir.

Tamsayı sayıları alan seçenekler ondalık, sekizlik veya onaltılık tabanda belirtilen değerleri kabul edebilir. Bir sayı 0x ile başladığında, onaltılık olarak ele alınacaktır; sadece 0 ile başladığında, sekizlik olarak ele alınacaktır. Aksi takdirde, Nping sayının 10 tabanında belirtildiğini varsayacaktır. Komut satırından sağlanabilecek hemen hemen tüm sayılar işaretsizdir, bu nedenle genel bir kural olarak minimum değer sıfırdır. Kullanıcılar ayrıca Nping'in beklenen aralıkta rastgele bir değer üretmesini sağlamak için random veya rand kelimesini de belirtebilirler.

IP adresleri IPv4 adresleri (örn. 192.168.1.1), IPv6 adresleri (örn. 2001:db8:85a3::8e4c:760:7146) veya ana bilgisayar sisteminde yapılandırılmış varsayılan DNS sunucusu kullanılarak çözümlenecek ana bilgisayar adları olarak verilebilir.

MAC adreslerini alan seçenekler normal iki nokta üst üste ayrılmış 6 hex bayt biçimini kabul eder (örn. 00:50:56:d4:01:98). İki nokta üst üste yerine kısa çizgi de kullanılabilir (örn. 00-50-56-c0-00-08). Random veya rand özel sözcüğü rastgele bir adres ayarlar ve broadcast veya bcast sözcüğü ff:ff:ff:ff:ff:ff ayarlar.

General Operation (Genel Çalışma)

Diğer ping ve paket oluşturma araçlarının aksine, Nping çoklu hedef ana bilgisayar ve bağlantı noktası özelliklerini destekler. Bu büyük bir esneklik sağlarken, Nping'in birden fazla ana bilgisayar ve/veya prob gönderilecek birden fazla portun olduğu durumları nasıl ele aldığı açık değildir. Bu bölüm Nping'in bu durumlarda nasıl davrandığını açıklamaktadır.

Birden fazla hedef ana bilgisayar belirtildiğinde, Nping bunlar arasında round-robin tarzında döner. Bu, yavaş ana bilgisayarlara başka bir sonda gönderilmeden önce yanıtlarını göndermeleri için daha fazla zaman verir. Portlar da round robin kullanılarak programlanır. Bu nedenle, yalnızca bir bağlantı noktası belirtilmediği sürece, Nping asla aynı hedef ana bilgisayara ve bağlantı noktasına art arda iki sonda göndermez.

Hedeflerin etrafındaki döngü "iç döngü" ve portların etrafındaki döngü "dış döngü "dür. Bir sonraki porta geçmeden önce tüm hedeflere belirli bir port için bir prob gönderilecektir. Problar arasında Nping, --delay seçeneği tarafından kontrol edilen

"problar arası gecikme" adı verilen yapılandırılabilir bir süre bekler. Bu örnekler nasıl çalıştığını göstermektedir.

Bir hedef, üç bağlantı noktası ve iki mermi.

```
# nping --tcp -c 2 1.1.1.1 -p 100-102

Starting Nping ( https://nmap.org/nping )
SENT (0.0210s) TCP 192.168.1.77 > 1.1.1.1:100
SENT (1.0230s) TCP 192.168.1.77 > 1.1.1.1:101
SENT (2.0250s) TCP 192.168.1.77 > 1.1.1.1:102
SENT (3.0280s) TCP 192.168.1.77 > 1.1.1.1:100
SENT (4.0300s) TCP 192.168.1.77 > 1.1.1.1:101
SENT (5.0320s) TCP 192.168.1.77 > 1.1.1.1:102
```

Üç hedef, bir liman ve iki mermi.

```
# nping --tcp -c 2 1.1.1.1 2.2.2.2 3.3.3.3 -p 8080

Starting Nping ( https://nmap.org/nping )
SENT (0.0230s) TCP 192.168.0.21 > 1.1.1.1:8080
SENT (1.0240s) TCP 192.168.0.21 > 2.2.2.2:8080
SENT (2.0260s) TCP 192.168.0.21 > 3.3.3.3:8080
SENT (3.0270s) TCP 192.168.0.21 > 1.1.1.1:8080
SENT (4.0290s) TCP 192.168.0.21 > 2.2.2.2:8080
SENT (5.0310s) TCP 192.168.0.21 > 3.3.3.3:8080
```

Üç ana bilgisayar, üç bağlantı noktası, bir tur, problar arası gecikme 500 ms.

```
# nping --tcp -c 1 --delay 500ms 1.1.1.1 2.2.2.2 3.3.3.3 -p 137-139

Starting Nping ( https://nmap.org/nping )
SENT (0.0230s) TCP 192.168.0.21 > 1.1.1.1:137
SENT (0.5250s) TCP 192.168.0.21 > 2.2.2.2:137
SENT (1.0250s) TCP 192.168.0.21 > 3.3.3.3:137
SENT (1.5280s) TCP 192.168.0.21 > 1.1.1.1:138
SENT (2.0280s) TCP 192.168.0.21 > 2.2.2.2:138
SENT (2.5310s) TCP 192.168.0.21 > 3.3.3.3:138
SENT (3.0300s) TCP 192.168.0.21 > 1.1.1.1:139
SENT (3.5330s) TCP 192.168.0.21 > 2.2.2.2:139
SENT (4.0330s) TCP 192.168.0.21 > 3.3.3.3:139
```

Probe Modes (Prob Modları)

Nping çok çeşitli protokolleri destekler. Bazı durumlarda Nping kullanılan seçeneklerden modu otomatik olarak belirleyebilse de, genellikle açıkça belirtmek iyi bir fikirdir.

`--tcp-connect` (TCP Connect mode) ⇒ TCP bağlantı modu, bir kullanıcının ham paket ayrıcalıklarına sahip olmadığı durumlarda varsayılan moddur. Nping, diğer modların çoğunun yaptığı gibi ham paketler yazmak yerine, temel işletim sisteminden connect sistem çağrısını yayınlayarak hedef makine ve bağlantı noktası ile bir bağlantı kurmasını ister. Bu, web tarayıcılarının, P2P istemcilerinin ve diğer ağ özellikli uygulamaların çoğunun bağlantı kurmak için kullandığı aynı üst düzey sistem çağrısıdır. Berkeley Sockets API olarak bilinen programlama arayüzünün bir parçasıdır. Nping, kablodan ham paket yanıtlarını okumak yerine, her bağlantı denemesinde durum bilgisi almak için bu API'yi kullanır. Bu nedenle, gönderilen veya alınan paketlerin içeriğini göremezsiniz, yalnızca gerçekleşen TCP bağlantı kuruluşuyla ilgili durum bilgilerini görebilirsiniz.

`--tcp` (TCP mode) ⇒ TCP, kullanıcıların her türlü TCP paketini oluşturmasına ve göndermesine olanak tanıyan moddur. TCP paketleri, ayarlanabilen IP paketlerine gömülü olarak gönderilir. Bu mod birçok farklı amaç için kullanılabilir. Örneğin, üç yönlü el sıkışmayı tamamlamadan TCP SYN mesajları göndererek açık portları keşfetmeye çalışabilirsiniz. Bu teknik genellikle yarı açık tarama olarak adlandırılır, çünkü tam bir TCP bağlantısı açmazsınız. Sanki gerçek bir bağlantı açacakmışsınız gibi bir SYN paketi gönderir ve ardından yanıt beklersiniz. Bir SYN/ACK portun açık olduğunu gösterirken, bir RST kapalı olduğunu gösterir. Herhangi bir yanıt alınmazsa, bazı ara ağ cihazlarının yanıtları filtrelediği varsayılabilir. Başka bir kullanım alanı da uzaktaki bir TCP/IP yığınının hem SYN hem de RST bayrakları ayarlanmış bir paket gibi RFC uyumlu olmayan bir paket aldığında nasıl davrandığını görmek olabilir. Ayrıca, aktif bir TCP bağlantısını kapatmak amacıyla sahte bir IP adresi kullanarak özel RST paketleri oluşturarak bazı kötülükler de yapılabilir.

`--udp` (UDP mode) ⇒ UDP modu iki farklı davranışa sahip olabilir. Normal şartlar altında, kullanıcıların özel IP/UDP paketleri oluşturmasına izin verir. Ancak, Nping ham paket ayrıcalıkları olmayan bir kullanıcı tarafından çalıştırılırsa ve varsayılan protokol başlıklarında herhangi bir değişiklik istenmezse, Nping temel olarak sendto sistem çağrısını kullanarak belirtilen hedef ana bilgisayarlara ve bağlantı

noktalarına UDP paketleri gönderen ayrıcalıksız UDP moduna girer. Bu ayrıcalıksız modda, kablodaki paketlerin düşük seviyeli başlık bilgilerini görmenin mümkün olmadığını, yalnızca iletilen ve alınan bayt miktarı hakkında durum bilgisi olduğunu unutmayın. UDP modu herhangi bir UDP tabanlı sunucu ile etkileşim kurmak için kullanılabilir. Örnek olarak DNS sunucuları, akış sunucuları, çevrimiçi oyun sunucuları ve port vurma/tek paket yetkilendirme daemonları verilebilir.

`--icmp` (ICMP mode) ⇒ ICMP modu, kullanıcı Nping'i ham paket ayrıcalıklarıyla çalıştırdığında varsayılan moddur. Her türlü ICMP mesajı oluşturulabilir. Varsayılan ICMP türü Echo, yani ping'dir. ICMP modu, basit bir zaman damgası veya ağ maskesi isteğinden sahte hedefe ulaşılamıyor mesajlarının, özel yönlendirmelerin ve yönlendirici reklamlarının iletilmesine kadar birçok farklı amaç için kullanılabilir.

`--arp` (ARP/RARP mode) ⇒ ARP, ARP ile ilgili birkaç farklı paket oluşturmanıza ve göndermenize olanak tanır. Bunlar ARP, RARP, DRARP ve InARP istek ve yanıtlarını içerir. Bu mod, düşük seviyeli ana bilgisayar keşfi gerçekleştirmek ve ARP önbelleği zehirleme saldırıları yapmak için yasaklanabilir.

`--traceroute` (Traceroute mode) ⇒ Traceroute kendi başına bir mod değildir ancak TCP, UDP ve ICMP modlarının tamamlayıcısıdır. Bu seçenek belirtildiğinde Nping ilk probun IP TTL değerini 1 olarak ayarlayacaktır. Bir sonraki yönlendirici paketi aldığında, TTL'nin sona ermesi nedeniyle paketi düşürecek ve bir ICMP hedefe ulaşılamıyor mesajı oluşturacaktır. Bir sonraki probun TTL değeri 2 olacaktır, bu nedenle şimdi ilk yönlendirici paketi iletirken, ikinci yönlendirici paketi düşüren ve ICMP mesajı üreten yönlendirici olacaktır. Üçüncü probun TTL değeri 3 olacaktır ve bu böyle devam edecektir. Tüm bu ICMP Destination Unreachable mesajlarının kaynak adreslerini inceleyerek, sondaların nihai hedeflerine ulaşana kadar izledikleri yolu belirlemek mümkündür.

TCP Connect Mode (TCP Bağlantı Modu)

`-p` *<port_spec>*, `--dest-port` *<port_spec>* (Target ports) ⇒ Bu seçenek hangi portlara bağlanmayı denemek istediğinizi belirtir. Tek bir port, virgülle ayrılmış bir port listesi (örn. 80,443,8080), bir aralık (örn. 1-1023) veya bunların herhangi bir kombinasyonu (örn. 21-25,80,443,1024-2048) olabilir. Bir aralığın başlangıç ve/veya bitiş değerleri atlanabilir, bu da Nping'in sırasıyla 1 ve 65535 değerlerini

kullanmasına neden olur. Böylece 1'den 65535'e kadar olan portları hedeflemek için -p- belirtebilirsiniz. Açıkça belirtmeniz halinde sıfır numaralı portun kullanılmasına izin verilir.

`-g` `<portnumber>`, `--source-port` `<portnumber>` (Spoof source port) ⇒ Bu seçenek Nping'den TCP bağlantıları için kaynak port olarak belirtilen portu kullanmasını ister. Bunun tüm sistemlerde çalışmayabileceğini veya root ayrıcalıkları gerektirebileceğini unutmayın. Belirtilen değer [0-65535] aralığında bir tamsayı olmalıdır.

TCP Mode (TCP Modu)

`-p` `<port_spec>`, `--dest-port` `<port_spec>` (Target ports) ⇒ Bu seçenek, probları hangi hedef portlara göndermek istediğinizi belirtir. Tek bir port, virgülle ayrılmış bir port listesi (örn. 80,443,8080), bir aralık (örn. 1-1023) veya bunların herhangi bir kombinasyonu (örn. 21-25,80,443,1024-2048) olabilir. Bir aralığın başlangıç ve/veya bitiş değerleri atlanabilir, bu da Nping'in sırasıyla 1 ve 65535 değerlerini kullanmasına neden olur. Böylece 1'den 65535'e kadar olan portları hedeflemek için -p- belirtebilirsiniz. Açıkça belirtmeniz halinde sıfır numaralı bağlantı noktasının kullanılmasına izin verilir.

`-g` `<portnumber>`, `--source-port` `<portnumber>` (Spoof source port) ⇒ Bu seçenek Nping'den TCP bağlantıları için kaynak port olarak belirtilen portu kullanmasını ister. Bunun tüm sistemlerde çalışmayabileceğini veya root ayrıcalıkları gerektirebileceğini unutmayın. Belirtilen değer [0-65535] aralığında bir tamsayı olmalıdır.

`--seq` `<seqnumber>` (Sequence Number) ⇒ TCP sıra numarasını belirtir. SYN paketlerinde bu, başlangıç sıra numarasıdır (ISN). Normal bir iletimde bu, segmentteki ilk veri baytının sıra numarasına karşılık gelir. <sıra numarası> [0-4294967295] aralığında bir sayı olmalıdır.

`--flags` `<flags>` (TCP Flags) ⇒ Bu seçenek TCP paketinde hangi bayrakların ayarlanması gerektiğini belirtir. <flags> üç farklı şekilde belirtilebilir:

1. Virgülle ayrılmış bir bayrak listesi olarak, örneğin --flags syn,ack,rst

2. Bir karakterlik bayrak baş harflerinin bir listesi olarak, örneğin --flags SAR Nping'e SYN, ACK ve RST bayraklarını ayarlamasını söyler.
3. 8 bitlik onaltılık bir sayı olarak, verilen sayı TCP başlığının flags alanına yerleştirilecek tam değerdir. Sayı 0x önekiyle başlamalı ve [0x00-0xFF] aralığında olmalıdır, örneğin --flags 0x20 URG bayrağını ayarlar, çünkü 0x20 ikili 00100000'a karşılık gelir ve URG bayrağı üçüncü bit ile temsil edilir.

Ayarlanabilecek 8 olası bayrak vardır: CWR, ECN, URG, ACK, PSH, RST, SYN ve FIN. ALL özel değeri tüm bayrakları ayarlamak anlamına gelir. NONE hiçbir bayrağın ayarlanmaması anlamına gelir. Herhangi bir bayrağın ayarlanmasını istemiyorsanız, bunu açıkça talep etmeniz önemlidir, çünkü bazı durumlarda SYN bayrağı varsayılan olarak ayarlanmış olabilir. Burada her bir bayrağın anlamının kısa bir açıklaması bulunmaktadır:

- CWR (Congestion Window Reduced) (Tıkanıklık Penceresi Azaltıldı) ⇒ ECN Yetenekli bir gönderici tarafından tıkanıklık penceresini azalttığında ayarlanır (bir yeniden iletim zaman aşımı, hızlı bir yeniden iletim nedeniyle veya bir ECN bildirimine yanıt olarak.
- ECN (Explicit Congestion Notification) (Açık Tıkanıklık Bildirimi) ⇒ Üç yönlü el sıkışma sırasında göndericinin açık tıkanıklık bildirimi yapabildiğini gösterir. Normalde, normal iletim sırasında IP Congestion Experienced bayrağı ayarlanmış bir paketin alındığı anlamına gelir. Daha fazla bilgi için RFC 3168'e bakın.
- URG (Urgent) ⇒ Segment acildir ve acil işaretçi alanı geçerli bilgi taşır.
- ACK (Acknowledgement) (Teşekkür) ⇒ Segment bir onay taşır ve onay numarası alanının değeri geçerlidir ve alıcıdan beklenen bir sonraki sıra numarasını içerir.
- PSH (Push) ⇒ Bu segmentteki veriler varışta hemen uygulama katmanına itilmelidir.
- RST (Reset) ⇒ Bir sorun oluştu ve gönderici bağlantıyı iptal etmek istiyor.
- SYN (Synchronize) (Senkronize et) ⇒ Segment, sıra numaralarını senkronize etmek ve bir bağlantı kurmak için bir istektir. Sıra numarası alanı göndericinin ilk sıra numarasını içerir.
- FIN (Finish) (bitirmek) ⇒ Gönderici bağlantıyı kapatmak istiyor.

- `--win` `<size>` (Window Size) ⇒ TCP pencere boyutunu, yani segmentin göndericisinin alıcıdan tek seferde kabul etmek istediği sekizli sayısını belirtir. Bu genellikle işletim sisteminin belirli bir bağlantı için ayırdığı alım tamponunun boyutudur. <size> [0-65535] aralığında bir sayı olmalıdır.
- `--badsum` (Invalid Checksum) (Geçersiz Sağlama Toplamı) ⇒ Nping'den hedef ana bilgisayarlara gönderilen paketler için geçersiz bir TCP sağlama toplamı kullanmasını ister. Neredeyse tüm ana IP yığınları bu paketleri düzgün bir şekilde düşürdüğünden, alınan yanıtlar büyük olasılıkla sağlama toplamını doğrulama zahmetine girmeyen bir güvenlik duvarı veya IDS'den geliyordur. Bu teknik hakkında daha fazla bilgi için bkz. https://nmap.org/p60-12.html.

UDP Mode (UDP Modu)

`-p` `<port_spec>`, `--dest-port` `<port_spec>` (Target ports) ⇒ Bu seçenek UDP datagramlarının hangi portlara gönderilmesini istediğinizi belirtir. Tek bir port, virgülle ayrılmış bir port listesi (örn. 80,443,8080), bir aralık (örn. 1-1023) veya bunların herhangi bir kombinasyonu (örn. 21-25,80,443,1024-2048) olabilir. Bir aralığın başlangıç ve/veya bitiş değerleri atlanabilir, bu da Nping'in sırasıyla 1 ve 65535 değerlerini kullanmasına neden olur. Böylece 1'den 65535'e kadar olan portları hedeflemek için -p- belirtebilirsiniz. Açıkça belirtmeniz halinde sıfır numaralı bağlantı noktasının kullanılmasına izin verilir.

`-g` `<portnumber>`, `--source-port` `<portnumber>` (Spoof source port) ⇒ Bu seçenek Nping'den iletilen datagramlar için kaynak port olarak belirtilen portu kullanmasını ister. Bunun tüm sistemlerde çalışmayabileceğini veya root ayrıcalıkları gerektirebileceğini unutmayın. Belirtilen değer [0-65535] aralığında bir tamsayı olmalıdır.

`--badsum` (Invalid Checksum) ⇒ Nping'den hedef ana bilgisayarlara gönderilen paketler için geçersiz bir UDP sağlama toplamı kullanmasını ister. Neredeyse tüm ana IP yığınları bu paketleri düzgün bir şekilde düşürdüğünden, alınan yanıtlar büyük olasılıkla sağlama toplamını doğrulama zahmetine girmeyen bir güvenlik duvarı veya IDS'den geliyordur. Bu teknik hakkında daha fazla bilgi için bkz. https://nmap.org/p60-12.html.

ICMP Mode (ICMP Modu)

`--icmp-type` `<type>` (ICMP type) ⇒ Bu seçenek hangi tür ICMP mesajlarının oluşturulacağını belirtir. <type> iki farklı şekilde sağlanabilir. IANA tarafından atanan resmi tür numaralarını kullanabilirsiniz (örneğin, ICMP Yankı İsteği için --icmp-type 8) veya "ICMP Türleri" adlı bölümde listelenen anımsatıcılardan herhangi birini kullanabilirsiniz.

`--icmp-code` `<code>` (ICMP code) ⇒ This option specifies which ICMP code should be included in the generated ICMP messages. <code> can be supplied in two different ways. You can use the official code numbers assigned by IANA (e.g. --icmp-code 1 for Fragment Reassembly Time Exceeded), or you can use any of the mnemonics listed in the section called “ICMP Codes”.

`--icmp-id` `<id>` (ICMP identifier) ⇒ Bu seçenek, bazı ICMP mesajlarında kullanılan tanımlayıcının değerini belirtir. Genel olarak istek ve yanıt iletilerini eşleştirmek için kullanılır. <id> [0-65535] aralığında bir sayı olmalıdır.

`--icmp-seq` `<seq>` (ICMP sequence) ⇒ Bu seçenek, bazı ICMP iletilerinde kullanılan sıra numarası alanının değerini belirtir. Genel olarak istek ve yanıt iletilerini eşleştirmek için kullanılır. <id> [0-65535] aralığında bir sayı olmalıdır.

`--icmp-redirect-addr` `<addr>` (ICMP Redirect address) ⇒ Bu seçenek ICMP Yönlendirme iletilerindeki adres alanını ayarlar. Başka bir deyişle, IP datagramlarını orijinal hedefe gönderirken kullanılması gereken yönlendiricinin IP adresini ayarlar. <addr> bir IPv4 adresi ya da bir ana bilgisayar adı olabilir.

`--icmp-param-pointer` `<pointer>` (ICMP Parameter Problem pointer) ⇒ Bu seçenek, ICMP Parametre Sorunu iletilerinde sorunun yerini gösteren işaretçiyi belirtir. <pointer> [0-255] aralığında bir sayı olmalıdır. Normalde bu seçenek yalnızca ICMP kodu 0 olarak ayarlandığında kullanılır ("İşaretçi hatayı gösterir").

`--icmp-advert-lifetime` `<ttl>` (ICMP Router Advertisement Lifetime) ⇒ Bu seçenek, yönlendirici reklamı ömrünü, yani bir ICMP Yönlendirici Reklamında taşınan bilginin geçerli sayılabileceği saniye sayısını belirtir. <ttl> [0-65535] aralığında pozitif bir tamsayı olmalıdır.

`--icmp-advert-entry` `<addr>` , `<pref>` (ICMP Router Advertisement Entry) ⇒ Bu seçenek, ICMP Yönlendirici Reklamı mesajına bir Yönlendirici Reklamı girişi ekler. Parametre virgülle ayrılmış iki değerden oluşmalıdır. <addr> yönlendiricinin IP'sidir ve nokta ondalık gösterimde bir IP adresi veya bir ana bilgisayar adı olarak belirtilebilir. <pref> belirtilen IP için tercih düzeyidir. 0-4294967295] aralığında bir sayı olmalıdır. Örnek olarak --icmp-advert-entry 192.168.128.1,3 verilebilir.

`--icmp-orig-time` `<timestamp>` (ICMP Originate Timestamp) ⇒ Bu seçenek, ICMP Zaman Damgası iletilerindeki Kaynak Zaman Damgasını ayarlar. Başlangıç Zaman Damgası, UTC gece yarısından bu yana geçen milisaniye sayısı olarak ifade edilir ve göndericinin Zaman Damgası iletisine iletilmeden önce en son dokunduğu zamana karşılık gelir. <timestamp> normal bir zaman (örneğin 10s, 3h, 1000ms) veya şimdi özel dizesi olarak belirtilebilir. Örneğin --icmp-orig-time now-2s, --icmp-orig-time now+1h, --icmp-orig-time now+200ms gibi now değerlerine ekleme veya çıkarma yapabilirsiniz.

`--icmp-recv-time` `<timestamp>` (ICMP Receive Timestamp) ⇒ Bu seçenek ICMP Zaman Damgası mesajlarındaki Alma Zaman Damgasını ayarlar. Alma Zaman Damgası, UTC gece yarısından itibaren milisaniye sayısı olarak ifade edilir ve yankılayıcının Zaman Damgası iletisini aldıktan sonra ilk dokunduğu zamana karşılık gelir. <timestamp>, --icmp-orig-time ile olduğu gibidir.

`--icmp-trans-time` `<timestamp>` (ICMP Transmit Timestamp) ⇒ Bu seçenek ICMP Zaman Damgası mesajlarında İletim Zaman Damgasını ayarlar. İletim Zaman Damgası, UTC gece yarısından itibaren milisaniye sayısı olarak ifade edilir ve yankılayıcının iletilmeden önce Zaman Damgası mesajına en son dokunduğu zamana karşılık gelir. <timestamp>, --icmp-orig-time ile olduğu gibidir.

ICMP Types (ICMP türleri)

Bu tanımlayıcılar --icmp-type seçeneğinde verilen ICMP tip numaraları için anımsatıcı olarak kullanılabilir. Genel olarak her tanımlayıcının üç biçimi vardır: tam ad (örn. destination-unreachable), kısa ad (örn. dest-unr) veya baş harfler (örn. du). Bir şey talep eden ICMP türlerinde "talep" kelimesi atlanır.

`echo-reply` , `echo-rep` , `er` ⇒ Yankı Yanıtı (tip 0). Bu mesaj bir Yankı İsteği mesajına yanıt olarak gönderilir.

`destination-unreachable` , `dest-unr` , `du` ⇒ Hedefe Ulaşılamıyor (tip 3). Bu mesaj, bir datagramın hedefine teslim edilemediğini gösterir.

`source-quench`, `sour-que`, `sq` ⇒ Kaynak Söndürme (tip 4). Bu mesaj, sıkışık bir IP cihazı tarafından diğer cihaza paketleri çok hızlı gönderdiğini ve yavaşlaması gerektiğini söylemek için kullanılır.

`redirect`, `redi`, `r` ⇒ Yönlendirme (tip 5). Bu mesaj normalde yönlendiriciler tarafından bir ana bilgisayara datagram göndermek için kullanılacak daha iyi bir yol olduğunu bildirmek için kullanılır. Ayrıca --icmp-redirect-addr seçeneğine de bakın.

`echo-request`, `echo`, `e` ⇒ Yankı İsteği (tip 8). Bu mesaj, ağ üzerindeki başka bir cihazın bağlantısını test etmek için kullanılır.

`router-advertisement`, `rout-adv`, `ra` ⇒ Yönlendirici Reklamı (tip 9). Bu mesaj yönlendiriciler tarafından ana bilgisayarlara varlıklarını ve yeteneklerini bildirmek için kullanılır. Ayrıca --icmp-advert-lifetime seçeneğine de bakın.

`router-solicitation`, `rout-sol`, `rs` ⇒ Yönlendirici İsteği (tip 10). Bu mesaj, ana bilgisayarlar tarafından dinleyen yönlendiricilerden Yönlendirici Reklamı mesajları istemek için kullanılır.

`time-exceeded`, `time-exc`, `te` ⇒ Zaman Aşıldı (tip 11). Bu mesaj, IP TTL süresi dolduğu için bir datagramın hedefine ulaşmadan atıldığını belirtmek için bazı ara cihazlar (normalde bir yönlendirici) tarafından oluşturulur.

`parameter-problem`, `member-pro`, `pp` ⇒ Parametre Sorunu (tip 12). Bu ileti, bir aygıt IP başlığındaki bir parametreyle ilgili bir sorun bulduğunda ve bunu işlemeye devam edemediğinde kullanılır. Ayrıca --icmp-param-pointer seçeneğine de bakın.

`timestamp`, `time`, `tm` ⇒ Zaman Damgası İsteği (tip 13). Bu mesaj, bir cihazdan yayılma süresi hesaplaması ve saat senkronizasyonu için bir zaman damgası değeri göndermesini istemek için kullanılır. Ayrıca --icmp-orig-time, --icmp-recv-time ve --icmp-trans-time iletilerine de bakın.

`timestamp-reply`, `time-rep`, `tr` ⇒ Zaman Damgası Yanıtı (tip 14). Bu mesaj bir Zaman Damgası İstek mesajına yanıt olarak gönderilir.

`information`, `info`, `i` ⇒ Bilgi Talebi (tip 15). Bu mesaj artık kullanılmamaktadır, ancak orijinal olarak başka bir cihazdan yapılandırma bilgisi istemek için kullanılmıştır.

`information-reply`, `info-rep`, `ir` ⇒ Bilgi Yanıtı (tip 16). Bu mesaj artık kullanılmamaktadır, ancak başlangıçta yapılandırma bilgisi sağlamak için bir Bilgi İsteği mesajına yanıt olarak gönderilmiştir.

`mask-request`, `mask`, `m` ⇒ Adres Maskesi İsteği (tip 17). Bu mesaj, bir cihazdan alt ağ maskesini göndermesini istemek için kullanılır.

`mask-reply`, `mask-rep`, `mr` ⇒ Adres Maskesi Yanıtı (tip 18). Bu mesaj bir alt ağ maskesi içerir ve bir Adres Maskesi İstek mesajına yanıt olarak gönderilir.

`traceroute`, `trace`, `tc` ⇒ Traceroute (tip 30). Bu mesaj normalde bir ara cihaz tarafından traceroute seçeneği olan bir IP datagramı aldığında gönderilir. ICMP Traceroute mesajları hala deneyseldir, daha fazla bilgi için RFC 1393'e bakın.

ICMP Codes (ICMP Kodları)

Bu tanımlayıcılar --icmp-code seçeneğinde verilen ICMP kod numaraları için anımsatıcı olarak kullanılabilir. Bunlar karşılık geldikleri ICMP türüne göre listelenmiştir.

Hedefe Ulaşılamıyor

`network-unreachable`, `netw-unr`, `net` ⇒ Kod 0. Datagram hedef ağına teslim edilemedi (muhtemelen bazı yönlendirme sorunları nedeniyle).

`host-unreachable`, `host-unr`, `host` ⇒ Kod 1. Datagram hedef ağa teslim edildi ancak belirtilen ana bilgisayara ulaşmak imkansızdı (muhtemelen bazı yönlendirme sorunları nedeniyle).

`protocol-unreachable`, `prot-unr`, `proto` ⇒ Kod 2. IP datagramının Protokol alanında belirtilen protokol, datagramın teslim edildiği ana bilgisayar tarafından desteklenmiyor.

`port-unreachable`, `port-unr`, `port` ⇒ Kod 3. TCP/UDP hedef bağlantı noktası geçersizdi.

`needs-fragmentation`, `need-fra`, `frag` ⇒ Kod 4. Datagramın DF biti ayarlanmıştı ancak bir sonraki fiziksel ağın MTU'su için çok büyüktü, bu nedenle düşürülmesi gerekiyordu.

`source-route-failed`, `sour-rou`, `routefail` ⇒ Kod 5. IP datagramının Kaynak Rota seçeneği vardı ancak bir yönlendirici bunu bir sonraki atlamaya aktaramadı.

`network-unknown`, `netw-unk`, `net?` ⇒ Kod 6. Hedef ağ bilinmiyor. Bu kod asla kullanılmaz. Bunun yerine Ağa Erişilemiyor kullanılır.

`host-unknown`, `host-unk`, `host?` ⇒ Kod 7. Belirtilen ana bilgisayar bilinmiyor. Genellikle kötü bir adresi bildirmek için hedef ana bilgisayara yerel bir yönlendirici tarafından oluşturulur.

`host-isolated`, `host-iso`, `isolated` ⇒ Kod 8. Kaynak Ana Bilgisayar İzole Edildi. Kullanılmıyor.

`network-prohibited`, `netw-pro`, `!net` ⇒ Kod 9. Hedef ağ ile iletişim idari olarak yasaklanmıştır (kaynak cihazın hedef ağa paket göndermesine izin verilmez).

`host-prohibited`, `host-pro`, `!host` ⇒ Kod 10. Hedef ana bilgisayarla iletişim idari olarak yasaklanmıştır. (Kaynak cihazın hedef ağa paket göndermesine izin verilir ancak hedef cihaza gönderilmesine izin verilmez).

`network-tos`, `unreachable-network-tos`, `netw-tos`, `tosnet` ⇒ Kod 11. IP TOS alanında belirtilen hizmet türünü sağlayamadığı için hedef ağa ulaşılamıyor.

`host-tos`, `unreachable-host-tos`, `toshost` ⇒ Kod 12. IP TOS alanında belirtilen hizmet türünü sağlayamadığı için hedef ana bilgisayara erişilemiyor.

`communication-prohibited`, `comm-pro`, `!comm` ⇒ Kod 13. İletiyi içeriğine göre engelleyen filtreleme nedeniyle datagram iletilemedi.

`host-precedence-violation`, `precedence-violation`, `prec-vio`, `violation` ⇒ Kod 14. IP TOS alanındaki öncelik değerine izin verilmez.

`precedence-cutoff`, `prec-cut`, `cutoff` ⇒ Kod 15. IP TOS alanındaki öncelik değeri ağ için izin verilen minimum değerden düşük.

Redirect ()

`redirect-network`, `redi-net`, `net` ⇒ Kod 0. Orijinal datagram ile aynı hedef ağa sahip gelecekteki tüm datagramları Adres alanında belirtilen yönlendiriciye yönlendirir. Bu kodun kullanımı RFC 1812 tarafından yasaklanmıştır.

`redirect-host`, `redi-host`, `host` ⇒ Kod 1. Orijinal datagram ile aynı hedef ana bilgisayara sahip gelecekteki tüm datagramları Adres alanında belirtilen yönlendiriciye yönlendirir.

`redirect-network-tos`, `redi-ntos`, `redir-ntos` ⇒ Kod 2. Orijinal datagram ile aynı hedef ağa ve IP TOS değerine sahip gelecekteki tüm datagramları Adres alanında belirtilen yönlendiriciye yönlendirin. Bu kodun kullanımı RFC 1812 tarafından yasaklanmıştır.

`redirect-host-tos`, `redi-htos`, `redir-htos` ⇒ Kod 3. Orijinal datagramla aynı hedef ana bilgisayara ve IP TOS değerine sahip gelecekteki tüm datagramları Adres alanında belirtilen yönlendiriciye yönlendirin.

Router Advertisement (Yönlendirici Reklamı)

`normal-advertisement`, `norm-adv`, `normal`, `zero`, `default`, `def` ⇒ Kod 0. Normal yönlendirici reklamı. Mobil IP'de: Mobilite aracısı, mobil düğümlerle ilgili olmayan IP datagramları için bir yönlendirici olarak hareket edebilir.

`not-route-common-traffic`, `not-rou`, `mobile-ip`, `!route`, `!commontraffic` ⇒ Kod 16. Mobil IP için kullanılır. Mobilite aracısı ortak trafiği yönlendirmez. Tüm yabancı aracılar, kayıtlı bir mobil düğümden alınan tüm datagramları varsayılan bir yönlendiriciye iletmelidir

Time Exceeded (Aşılan Süre)

`ttl-exceeded-in-transit`, `ttl-exc`, `ttl-transit` ⇒ Kod 0. IP Yaşam Süresi aktarım sırasında sona erdi.

`fragment-reassembly-time-exceeded`, `frag-exc`, `frag-time` ⇒ Kod 1. Parça yeniden birleştirme süresi aşıldı.

Parameter Problem (Parametre sorunu)

`pointer-indicates-error`, `poin-ind`, `pointer` ⇒ Kod 0. İşaretçi alanı sorunun yerini gösterir. Bkz. --icmp-param-pointer seçeneği.

`missing-required-option`, `miss-option`, `option-missing` ⇒ Kod 1. IP datagramının mevcut olmayan bir seçeneğe sahip olması bekleniyordu.

`bad-length`, `bad-len`, `badlen` ⇒ Kod 2. IP datagramının uzunluğu yanlış.

ARP Mode (ARP Modu)

`-arp-type` *`<type>`* (ICMP Type) ⇒ Bu seçenek hangi tür ARP mesajlarının oluşturulacağını belirtir. <type> iki farklı şekilde verilebilir. IANA tarafından atanan resmi numaraları kullanabilirsiniz (örneğin, ARP İsteği için --arp-type 1) veya "ARP Türleri" adlı bölümdeki anımsatıcılardan birini kullanabilirsiniz.

`--arp-sender-mac` *`<mac>`* (Sender MAC address) ⇒ Bu seçenek ARP başlığının Gönderen Donanım Adresi alanını ayarlar. ARP birçok bağlantı katmanı adresi türünü desteklese de, şu anda Nping yalnızca MAC adreslerini desteklemektedir. <mac> geleneksel MAC gösterimi kullanılarak belirtilmelidir (örn. 00:0a:8a:32:f4:ae). Ayırıcı olarak kısa çizgiler de kullanabilirsiniz (örn. 00-0a-8a-32-f4-ae).

`--arp-sender-ip` `<addr>` (Sender IP address) ⇒ Bu seçenek ARP başlığının Gönderen IP alanını ayarlar. <addr> bir IPv4 adresi veya bir ana bilgisayar adı olarak verilebilir.

`--arp-target-mac` `<mac>` (target MAC address) ⇒ Bu seçenek ARP başlığının Hedef Donanım Adresi alanını ayarlar.

`--arp-target-ip` `<addr>` (target ip address) ⇒ Bu seçenek ARP başlığının Hedef IP alanını ayarlar.

ARP Types (ARP Türleri)

Bu tanımlayıcılar --arp-type seçeneğine verilen ARP tipi numaraları için anımsatıcı olarak kullanılabilir.

`arp-request`, `arp`, `a` ⇒ ARP İsteği (tip 1). ARP istekleri, ağ katmanı adreslerini (normalde IP adresleri) bağlantı katmanı adreslerine (genellikle MAC adresleri) çevirmek için kullanılır. Temel olarak ARP isteği, belirli bir IP adresine sahip aynı ağ kesimindeki ana bilgisayardan MAC adresini vermesini isteyen yayınlanmış bir mesajdır.

`arp-reply`, `arp-rep`, `ar` ⇒ ARP Yanıtı (tip 2). ARP yanıtı, bir ana bilgisayarın bağlantı katmanı adresini sağlamak için bir ARP isteğine yanıt olarak gönderdiği bir mesajdır.

`rarp-request`, `rarp`, `r` ⇒ RARP İstekleri (tip 3). RARP istekleri, bir bağlantı katmanı adresini (normalde bir MAC adresi) bir ağ katmanı adresine (genellikle bir IP adresi) çevirmek için kullanılır. Temel olarak bir RARP isteği, kendi IP adresini bilmek isteyen bir ana bilgisayar tarafından gönderilen yayınlanmış bir mesajdır, çünkü herhangi bir IP adresi yoktur. Bootstrapping sorununu çözmek için tasarlanmış ilk protokoldür. Ancak, RARP artık kullanılmamaktadır ve bunun yerine DHCP kullanılmaktadır. RARP hakkında daha fazla bilgi için RFC 903'e bakın.

`rarp-reply`, `rarp-rep`, `rr` ⇒ RARP Yanıtı (tip 4). RARP yanıtı, ilk etapta RARP isteğini gönderen ana bilgisayara bir IP adresi sağlamak için bir RARP isteğine yanıt olarak gönderilen bir mesajdır.

`drarp-request`, `drarp`, `d` ⇒ Dinamik RARP İsteği (tip 5). Dinamik RARP, sabit bir bağlantı katmanı adresinden bir ağ katmanı adresi almak veya atamak için kullanılan bir RARP uzantısıdır. DRARP 90'lı yılların sonlarında çoğunlukla Sun Microsystems platformlarında kullanılmaktaydı ancak artık kullanılmamaktadır. Daha fazla bilgi için RFC 1931'e bakınız.

`drarp-reply`, `drarp-rep`, `dr` ⇒ Dinamik RARP Yanıtı (tip 6). DRARP yanıtı, ağ katmanı adresi sağlamak için bir RARP isteğine yanıt olarak gönderilen bir mesajdır.

`drarp-error`, `drarp-err`, `de` ⇒ DRARP Hatası (tip 7). DRARP Hata mesajları genellikle bir hatayı bildirmek için DRARP isteklerine yanıt olarak gönderilir. DRARP Hata mesajlarında, Hedef Protokol Adresi alanı bir hata kodu (genellikle ilk baytta) taşımak için kullanılır. Hata kodu, neden hiçbir hedef protokol adresinin döndürülmediğini anlatmak içindir. Daha fazla bilgi için RFC 1931'e bakın.

`inarp-request`, `inarp`, `i` ⇒ Ters ARP İsteği (tip 8). InARP istekleri, bir bağlantı katmanı adresini bir ağ katmanı adresine çevirmek için kullanılır. RARP isteğine benzer, ancak bu durumda InARP isteğini gönderen kendi adresini değil, başka bir düğümün ağ katmanı adresini bilmek ister. InARP esas olarak Frame Relay ve ATM ağlarında kullanılır. Daha fazla bilgi için RFC 2390'a bakın.

`inarp-reply`, `inarp-rep`, `ir` ⇒ Ters ARP Yanıtı (tip 9). InARP yanıt iletileri, belirli bir bağlantı katmanı adresine sahip ana bilgisayarla ilişkili ağ katmanı adresini sağlamak için InARP isteklerine yanıt olarak gönderilir.

`arp-nak`, `an` ⇒ ARP NAK (tip 10). ARP NAK mesajları ATMARP protokolünün bir uzantısıdır ve ATMARP sunucu mekanizmasının sağlamlığını artırmak için kullanılır. ARP NAK ile bir istemci, yıkıcı bir sunucu hatası ile ATMARP tablo arama hatası arasındaki farkı belirleyebilir. Daha fazla bilgi için RFC 1577'ye bakın.

IPv4 Options (IPv4 Seçenekleri)

`-S <addr>`, `--source-ip <addr>` (Source IP Address) ⇒ Kaynak IP adresini ayarlar. Bu seçenek, gönderilen paketlerde kaynak IP adresi olarak kullanılmak üzere özel bir IP adresi belirlemenizi sağlar. Bu, paketlerin göndericisinin taklit edilmesine olanak tanır. <addr> bir IPv4 adresi veya bir ana bilgisayar adı olabilir.

`--dest-ip <addr>` (Destination IP Address) ⇒ Nping'in hedef listesine bir hedef ekler. Bu seçenek tutarlılık için sağlanmıştır, ancak kullanımı düz hedef belirtimleri lehine kullanımdan kaldırılmıştır. "Hedef Belirtimi" adlı bölüme bakınız.

`--tos <tos>` (Type of Service) ⇒ IP TOS alanını ayarlar. TOS alanı, hizmet kalitesi özellikleri sağlamak üzere bilgi taşımak için kullanılır. Normalde Farklılaştırılmış

Hizmetler adı verilen bir tekniği desteklemek için kullanılır. Daha fazla bilgi için RFC 2474'e bakın. <tos> [0-255] aralığında bir sayı olmalıdır.

`--id` `<id>` (Identification) ⇒ IPv4 Kimlik alanını ayarlar. Kimlik alanı, belirli bir iletiye ait tüm parçalar için ortak olan 16 bitlik bir değerdir. Değer, alıcı tarafından alınan parçalardan orijinal mesajı yeniden birleştirmek için kullanılır. <id> [0-65535] aralığında bir sayı olmalıdır.

`--df` (Don't Fragment) ⇒ Gönderilen paketlerde Don't Fragment bitini ayarlar. Bir IP datagramının DF bayrağı ayarlandığında, ara cihazların onu parçalamasına izin verilmez, bu nedenle datagram uzunluğundan daha küçük bir MTU'ya sahip bir ağ üzerinden seyahat etmesi gerekiyorsa, datagramın düşürülmesi gerekecektir. Normalde bir ICMP Destination Unreachable mesajı oluşturulur ve gönderene geri gönderilir.

`--mf` (More Fragments) ⇒ Gönderilen paketlerde Diğer Parçalar bitini ayarlar. MF bayrağı, alıcıya geçerli datagramın daha büyük bir datagramın parçası olduğunu belirtmek için ayarlanır. Sıfıra ayarlandığında, geçerli datagramın kümedeki son parça ya da tek parça olduğunu gösterir.

`--evil` (Reserved / Evil) ⇒ Gönderilen paketlerdeki Ayrılmış / Kötü bitini ayarlar. Evil bayrağı, güvenlik duvarlarının ve diğer ağ güvenlik sistemlerinin kötü niyetli datagramlar ile yalnızca olağandışı olanları ayırt etmesine yardımcı olur. Ayarlandığında, datagramın kötü niyetli olduğunu gösterir ve güvensiz sistemlere boyun eğmeleri talimatını verir. Sıfır olarak ayarlanması kötü niyet olmadığını gösterir. SCRIPT_KIDDIE çevresel değişkeni sıfır olmayan bir değere ayarlanmışsa bu seçenek ima edilir.

`--ttl` `<hops>` (Time To Live) ⇒ Gönderilen paketlerdeki IPv4 Time-To-Live (TTL) alanını verilen değere ayarlar. TTL alanı, datagramın ağ üzerinde ne kadar süreyle var olmasına izin verildiğini belirtir. Başlangıçta bir saniye sayısını temsil etmesi amaçlanmıştır, ancak aslında bir paketin düşürülmeden önce geçebileceği atlama sayısını temsil eder. TTL, teslim edilemeyen datagramların bir yönlendiriciden diğerine sonsuza kadar iletilmeye devam ettiği bir durumdan kaçınmaya çalışır. <hops> [0-255] aralığında bir sayı olmalıdır.

`--badsum-ip` (Invalid IP checksum) ⇒ Nping'den hedef konaklara gönderilen paketler için geçersiz bir IP sağlama toplamı kullanmasını ister. Bazı sistemlerin (çoğu Linux çekirdeği gibi), paketi kabloya yerleştirmeden önce sağlama toplamını

düzeltebileceğini unutmayın, bu nedenle Nping çıktısında yanlış sağlama toplamını gösterse bile, paketler çekirdek tarafından şeffaf bir şekilde düzeltilebilir.

`--ip-options` `<R|S [route]|L [route]|T|U ...>` , `--ip-options` `<hex string>` (IP Options) ⇒ IP protokolü, paket başlıklarına yerleştirilebilecek çeşitli seçenekler sunar. Her yerde bulunan TCP seçeneklerinin aksine, IP seçenekleri pratiklik ve güvenlik kaygıları nedeniyle nadiren görülür. Aslında, birçok İnternet yönlendiricisi kaynak yönlendirme gibi en tehlikeli seçenekleri engeller. Yine de seçenekler bazı durumlarda hedef makinelere giden ağ rotasını belirlemek ve değiştirmek için yararlı olabilir. Örneğin, daha geleneksel traceroute tarzı yaklaşımlar başarısız olduğunda bile bir hedefe giden yolu belirlemek için record route seçeneğini kullanabilirsiniz. Ya da paketleriniz belirli bir güvenlik duvarı tarafından düşürülüyorsa, sıkı veya gevşek kaynak yönlendirme seçenekleriyle farklı bir rota belirleyebilirsiniz.

IP seçeneklerini belirtmenin en güçlü yolu --ip-options'a argüman olarak onaltılık verileri iletmektir. Her hex bayt değerinin önüne \x koyun. Belirli karakterleri bir yıldız işareti ve ardından tekrarlanmasını istediğiniz sayı ile takip ederek tekrarlayabilirsiniz. Örneğin, \x01\x07\x04\x00*4, \x01\x07\x04\x00\x00\x00\x00\x00 ile aynıdır.

Dördün katı olmayan bir bayt sayısı belirtirseniz, IP paketinde yanlış bir IP başlık uzunluğu ayarlanacağını unutmayın. Bunun nedeni, IP başlık uzunluğu alanının yalnızca dördün katlarını ifade edebilmesidir. Bu gibi durumlarda uzunluk, başlık uzunluğunun 4'e bölünmesi ve aşağı yuvarlanmasıyla hesaplanır. Bu, IP başlığını takip eden başlığın yorumlanma şeklini etkileyecek ve Nping'de veya herhangi bir sniffer çıktısında sahte bilgi gösterecektir. Bu tür bir durum bazı yığın stres testleri için yararlı olsa da, kullanıcılar normalde doğru başlık uzunluğunun ayarlanması için açık dolgu belirtmek isteyeceklerdir.

Nping ayrıca seçenekleri belirtmek için bir kısayol mekanizması sunar. Sırasıyla kayıt-yol, kayıt-zaman damgası veya her iki seçeneği birlikte istemek için R, T veya U harfini geçirmeniz yeterlidir. Gevşek veya katı kaynak yönlendirme, bir L veya S ve ardından bir boşluk ve ardından boşluk bırakılarak ayrılmış bir IP adresleri listesi ile belirtilebilir.

IP seçeneklerinin Nping ile kullanımına ilişkin daha fazla bilgi ve örnek için https://seclists.org/nmap-dev/2006/q3/0052.html adresindeki posta listesi gönderisine bakın.

`--mtu` `<size>` (Maximum Transmission Unit) ⇒ Bu seçenek, <size> değerinden büyük IP datagramlarının iletimden önce parçalanması için Nping'de kurgusal bir MTU ayarlar. <size> bayt olarak belirtilmelidir ve tek bir bağlantı katmanı çerçevesi üzerinde taşınabilecek sekizli sayısına karşılık gelir.

IPv6 Options (IPv6 Seçenekleri)

`-6`, `--ipv6` (Use IPv6) ⇒ Nping'e varsayılan IPv4 yerine IP sürüm 6'yı kullanmasını söyler. Bu seçeneği komut satırında mümkün olduğunca erken belirtmek genellikle iyi bir fikirdir, böylece Nping bunu kısa sürede ayrıştırabilir ve parametrelerin geri kalanının IPv6'ya atıfta bulunduğunu önceden bilebilir. Komut sözdizimi, -6 seçeneğini de eklemeniz dışında her zamanki gibidir. Elbette, bir ana bilgisayar adı yerine bir adres belirtirseniz IPv6 sözdizimini kullanmanız gerekir. Bir adres 3ffe:7501:4819:2000:210:f3ff:fe03:14d0 gibi görünebilir, bu nedenle ana bilgisayar adları önerilir.

IPv6 dünyayı tam olarak kasıp kavurmamış olsa da, bazı (genellikle Asya) ülkelerde önemli ölçüde kullanılmaktadır ve çoğu modern işletim sistemi bunu desteklemektedir. IPv6 ile Nping kullanmak için, paketlerinizin hem kaynağı hem de hedefi IPv6 için yapılandırılmış olmalıdır. İSS'niz (çoğu gibi) size IPv6 adresleri tahsis etmiyorsa, ücretsiz tünel aracıları yaygın olarak mevcuttur ve Nping ile iyi çalışır. Ücretsiz IPv6 tünel aracısı hizmetini http://www.tunnelbroker.net adresinden kullanabilirsiniz.

IPv6 desteğinin hala oldukça deneysel olduğunu ve birçok mod ve seçeneğin bununla çalışmayabileceğini lütfen unutmayın.

`-S` `<addr>`, `--source-ip` `<addr>` (Source IP Address) ⇒ Kaynak IP adresini ayarlar. Bu seçenek, gönderilen paketlerde kaynak IP adresi olarak kullanılmak üzere özel bir IP adresi belirlemenizi sağlar. Bu, paketlerin göndericisinin taklit edilmesine olanak tanır. <addr> bir IPv6 adresi veya bir ana bilgisayar adı olabilir.

`--dest-ip` `<addr>` (Destination IP Address) ⇒ Nping'in hedef listesine bir hedef ekler. Bu seçenek tutarlılık için sağlanmıştır, ancak kullanımı düz hedef belirtimleri lehine kullanımdan kaldırılmıştır. "Hedef Belirtimi" adlı bölüme bakınız.

`--flow` `<label>` (Flow Label) ⇒ Sets the IPv6 Flow Label. The Flow Label field is 20 bits long and is intended to provide certain quality-of-service properties for real-time datagram delivery. However, it has not been widely adopted, and not all routers or endpoints support it. Check RFC 2460 for more information. <label> must be an integer in the range [0–1048575].

`--traffic-class` `<class>` (Traffic Class) ⇒ IPv6 Trafik Sınıfını ayarlar. Bu alan IPv4'teki TOS alanına benzer ve Farklılaştırılmış Hizmetler yöntemini sağlayarak, her atlamada akış başına durum ve sinyalleşmeye gerek kalmadan İnternet'te ölçeklenebilir hizmet ayrımını mümkün kılmayı amaçlar. Daha fazla bilgi için RFC 2474'e bakın. <class> [0-255] aralığında bir tamsayı olmalıdır.

`--hop-limit` `<hops>` (Hop Limit) ⇒ Gönderilen paketlerdeki IPv6 Atlama Sınırı alanını verilen değere ayarlar. Atlama Sınırı alanı, datagramın ağ üzerinde ne kadar süreyle bulunmasına izin verildiğini belirtir. Bir paketin düşürülmeden önce geçebileceği atlama sayısını temsil eder. IPv4'teki TTL'de olduğu gibi, IPv6 Atlama Sayısı Sınırı, teslim edilemeyen datagramların bir yönlendiriciden diğerine sonsuza kadar iletilmeye devam ettiği bir durumdan kaçınmaya çalışır. <hops> [0-255] aralığında bir sayı olmalıdır.

Ethernet Options (Ethernet Seçenekleri)

Çoğu durumda Nping paketleri ham IP seviyesinde gönderir. Bu, Nping'in kendi IP paketlerini oluşturduğu ve bunları ham bir soket üzerinden ilettiği anlamına gelir. Ancak bazı durumlarda paketleri ham Ethernet seviyesinde göndermek gerekebilir. Bu, örneğin Nping Windows altında çalıştırıldığında (Microsoft Windows XP SP2'den beri ham soket desteğini devre dışı bıraktığı için) veya Nping'den ARP paketleri göndermesi istendiğinde olur. Bazı durumlarda ethernet çerçeveleri oluşturmak gerektiğinden, Nping farklı alanları manipüle etmek için bazı seçenekler sunar.

`--dest-mac` `<mac>` (Ethernet Destination MAC Address) ⇒ Bu seçenek, giden Ethernet çerçevelerinde ayarlanması gereken hedef MAC adresini ayarlar. Bu, Nping'in bir sonraki atlamanın MAC adresini belirleyememesi durumunda veya probları yapılandırılmış varsayılan ağ geçidi dışındaki bir yönlendirici üzerinden yönlendirmek istediğinizde kullanışlıdır. MAC adresi, iki nokta üst üste ayrılmış altı

bayttan oluşan olağan biçime sahip olmalıdır, örneğin 00:50:56:d4:01:98. Alternatif olarak, iki nokta üst üste yerine kısa çizgiler de kullanılabilir. Rastgele bir adres oluşturmak için random veya rand, ff:ff:ff:ff:ff:ff kullanmak için broadcast veya bcast sözcüklerini kullanın. Sahte bir hedef MAC adresi ayarlarsanız, problarınız amaçlanan hedeflere ulaşamayabilir.

`--source-mac` `<mac>` (Ethernet Source MAC Address) ⇒ Bu seçenek, giden Ethernet çerçevelerinde ayarlanması gereken kaynak MAC adresini ayarlar. Bu, Nping'in ağ arayüzünüzün MAC adresini belirleyememesi durumunda veya ağ kartınızın gerçek adresini gizlerken ağa trafik enjekte etmek istediğinizde kullanışlıdır. Sözdizimi --dest-mac ile aynıdır. Sahte bir kaynak MAC adresi ayarlarsanız, prob yanıtları alamayabilirsiniz.

`--ether-type` `<type>` (Ethertype) ⇒ Bu seçenek ethernet çerçevesinin Ethertype alanını ayarlar. Ethertype, yükte hangi protokolün kapsüllendiğini belirtmek için kullanılır. <type> iki farklı şekilde verilebilir. IEEE tarafından listelenen resmi numaraları (örneğin, IP sürüm 4 için --ether-type 0x0800) veya "Ethernet Türleri" adlı bölümdeki anımsatıcılardan birini kullanabilirsiniz.

Ethernet Types (Ethernet Türleri)

Bu tanımlayıcılar --arp-type seçeneğine verilen Ethertype numaraları için anımsatıcı olarak kullanılabilir.

`ipv4`, `ip`, `4` ⇒ Internet Protokolü sürüm 4 (tip 0x0800).

`ipv6`, `6` ⇒ Internet Protokolü sürüm 6 (tip 0x86DD).

`arp` ⇒ Adres Çözümleme Protokolü (tip 0x0806).

`rarp` ⇒ Ters Adres Çözümleme Protokolü (tip 0x8035).

`frame-relay`, `frelay`, `fr` ⇒ Frame Relay (tip 0x0808).

`ppp` ⇒ Noktadan Noktaya Protokol (tip 0x880B).

`gsmp` ⇒ Genel Anahtar Yönetim Protokolü (tip 0x880C).

`mpls` ⇒ Çok Protokollü Etiket Anahtarlama (tip 0x8847).

`mps-ual`, `mps` ⇒ Yukarı Akış Atamalı Etiket ile Çok Protokollü Etiket Anahtarlama (tip 0x8848).

`mcap` ⇒ Çok Noktaya Yayın Kanal Tahsis Protokolü (tip 0x8861).

`pppoe-discovery`, `pppoe-d` ⇒ Ethernet üzerinden PPP Keşif Aşaması (tip 0x8863).

`pppoe-session`, `pppoe-s` ⇒ Ethernet üzerinden PPP Oturum Aşaması (tip 0x8864).

`ctag` ⇒ Müşteri VLAN Etiket Tipi (0x8100 tipi).

`epon` ⇒ Ethernet Pasif Optik Ağ (tip 0x8808).

`pbnac` ⇒ Bağlantı noktası tabanlı ağ erişim denetimi (tip 0x888E).

`stag` ⇒ Servis VLAN etiketi tanımlayıcısı (0x88A8 tipi).

`ethexp1` ⇒ Yerel Deneysel Ethertype 1 (tip 0x88B5).

`ethexp2` ⇒ Yerel Deneysel Ethertype 2 (tip 0x88B6).

`ethoui` ⇒ OUI Genişletilmiş Eter Tipi (0x88B7 tipi).

`preauth` ⇒ Ön Kimlik Doğrulama (tür 0x88C7).

`lldp` ⇒ Bağlantı Katmanı Keşif Protokolü (tip 0x88CC).

`mac-security`, `mac-sec`, `macsec` ⇒ Ortam Erişim Denetimi Güvenliği (tip 0x88E5).

`mvrp` ⇒ Çoklu VLAN Kayıt Protokolü (tip 0x88F5).

`mmrp` ⇒ Çoklu Çok Noktaya Yayın Kayıt Protokolü (tip 0x88F6).

`frrr` ⇒ Hızlı Dolaşım Uzak İsteği (tip 0x890D).

Payload Options (Payload Seçenekleri)

`--data` *`<hex string>`* (Append custom binary data to sent packets) ⇒ Bu seçenek, gönderilen paketlere yük olarak ikili veri eklemenizi sağlar. <hex string> aşağıdaki formatlardan herhangi birinde belirtilebilir: 0xAABBCCDDEEFF<...>, AABBCCDDEEFF<...> veya \xAA\xBB\xCC\xDD\xEE\xFF<...>. Kullanım örnekleri --data 0xdeadbeef ve --data \xCA\xFE\x09'dur. 0x00ff gibi bir sayı belirtirseniz bayt sırası dönüşümü yapılmayacağını unutmayın. Bilgileri alıcının beklediği bayt sırasına göre belirttiğinizden emin olun.

`--data-string` *`<string>`* (Append custom string to sent packets) ⇒ Bu seçenek, gönderilen paketlere yük olarak normal bir dize eklemenizi sağlar. <string> herhangi bir dize içerebilir. Ancak, bazı karakterlerin sisteminizin yerel ayarına bağlı olabileceğini ve alıcının aynı bilgiyi görmeyebileceğini unutmayın. Ayrıca,

dizeyi çift tırnak içine aldığınızdan ve kabuktaki tüm özel karakterlerden kaçtığınızdan emin olun. Örnek: --data-string "Jimmy Jazz...".

`--data-length` `<len>` (Append random data to sent packets) ⇒ Bu seçenek, gönderilen paketlere yük olarak <len> rastgele veri baytları eklemenizi sağlar. <len> [0-65400] aralığında bir tamsayı olmalıdır. Ancak, ağ MTU sınırlamaları nedeniyle paketleri iletmek mümkün olmayabileceğinden 1400'den yüksek değerler önerilmez.

Echo Mode (Echo Modu)

"Yankı Modu", Nping tarafından uygulanan ve kullanıcıların ağ paketlerinin kaynaklandığı ana bilgisayardan hedef makineye geçiş sırasında nasıl değiştiğini görmelerini sağlayan yeni bir tekniktir. Temel olarak, Echo modu Nping'i iki farklı parçaya dönüştürür: Echo sunucusu ve Echo istemcisi. Echo sunucusu, ağdan paketleri yakalama ve bir yan TCP kanalı aracılığıyla kaynak istemciye bir kopyasını gönderme ("eko") yeteneğine sahip bir ağ hizmetidir. Yankı istemcisi, bu tür ağ paketlerini üreten, sunucuya ileten ve daha önce Yankı sunucusu ile kurduğu bir yan TCP kanalı aracılığıyla yankılanmış sürümlerini alan kısımdır.

Bu şema, istemcinin gönderdiği paketler ile sunucu tarafından gerçekte alınan paketler arasındaki farkları görmesini sağlar. Sunucunun alınan paketlerin kopyalarını yan kanaldan geri göndermesiyle, NAT cihazları gibi şeyler istemci tarafından hemen fark edilir hale gelir, çünkü kaynak IP adresindeki (ve hatta belki de kaynak portundaki) değişiklikleri fark eder. Trafik şekillendirme, TCP pencere boyutlarını değiştirme veya ana bilgisayarlar arasında şeffaf bir şekilde TCP seçenekleri ekleme gibi diğer cihazlar da ortaya çıkar.

Yankı modu, yönlendirme ve güvenlik duvarı sorunlarını gidermek için de kullanışlıdır. Diğer şeylerin yanı sıra, Nping istemcisi tarafından oluşturulan trafiğin aktarım sırasında düşüp düşmediğini ve hedefine asla ulaşıp ulaşmadığını veya yanıtların kendisine geri dönmeyenler olup olmadığını belirlemek için kullanılabilir.

Dahili olarak, istemci ve sunucu, teknik özellikleri https://nmap.org/svn/nping/docs/EchoProtoRFC.txt adresinde bulunan Nping Echo

Protocol (NEP) kullanarak şifreli ve kimliği doğrulanmış bir kanal üzerinden iletişim kurar.

Aşağıdaki paragraflarda Nping'in Yankı modunda mevcut olan farklı seçenekler açıklanmaktadır.

`--ec` `<passphrase>`, `--echo-client` `<passphrase>` (Run Echo client) ⇒ Bu seçenek Nping'e bir Echo istemcisi olarak çalışmasını söyler. <passphrase>, belirli bir oturumda şifreleme ve kimlik doğrulama için gereken kriptografik anahtarları oluşturmak için kullanılan bir ASCII karakter dizisidir. Parola, sunucu tarafından da bilinen bir sır olmalıdır ve herhangi bir sayıda yazdırılabilir ASCII karakteri içerebilir. Boşluk veya özel karakterler içeren parolalar çift tırnak içine alınmalıdır.

- Nping'i bir Echo istemcisi olarak çalıştırırken, normal ham prob modlarındaki çoğu seçenek geçerlidir. İstemci, --tcp, --icmp veya --udp gibi bayraklar kullanılarak belirli problar gönderecek şekilde yapılandırılabilir. Protokol başlık alanları uygun seçenekler (örneğin --ttl, --seq, --icmp-type, vb.) kullanılarak normal şekilde değiştirilebilir. Tek istisna ARP ile ilgili bayraklardır ve ARP gibi protokoller veri bağlantı katmanıyla yakından ilişkili olduğundan ve probları farklı ağ segmentlerinden geçemediğinden Echo modunda desteklenmez.

`--es` `<passphrase>`, `--echo-server` `<passphrase>` (Run Echo server) ⇒ Bu seçenek Nping'e bir Echo sunucusu olarak çalışmasını söyler. <passphrase>, belirli bir oturumda şifreleme ve kimlik doğrulama için gereken kriptografik anahtarları oluşturmak için kullanılan bir ASCII karakter dizisidir. Parola, istemciler tarafından da bilinen bir sır olmalıdır ve herhangi bir sayıda yazdırılabilir ASCII karakteri içerebilir. Boşluk veya özel karakterler içeren parolalar çift tırnak içine alınmalıdır. Tavsiye edilmemesine rağmen, --echo-server "" seçeneğini kullanarak boş parolalar kullanmanın mümkün olduğunu unutmayın. Ancak, istediğiniz şey açık bir Echo sunucusu kurmaksa, --no-crypto seçeneğini kullanmak daha iyidir. Ayrıntılar için aşağıya bakınız.

`--ep` `<port>`, `--echo-port` `<port>` (Set Echo TCP port number) ⇒ Bu seçenek Nping'den Echo yan kanal bağlantısı için belirtilen TCP port numarasını kullanmasını ister. Bu seçenek --echo-server ile birlikte kullanılırsa, sunucunun bağlantıları dinlediği portu belirtir. Eğer --echo-client ile birlikte kullanılırsa, uzak ana bilgisayarda bağlanılacak portu belirtir. Varsayılan olarak 9929 numaralı bağlantı noktası kullanılır.

`--nc` , `--no-crypto` (Disable encryption and authentication) ⇒ Bu seçenek Nping'den bir Echo oturumu sırasında herhangi bir kriptografik işlem kullanmamasını ister. Pratikte bu, Echo yan kanal oturum verilerinin açık olarak iletileceği ve oturum oluşturma aşamasında sunucu veya istemci tarafından herhangi bir kimlik doğrulama yapılmayacağı anlamına gelir. --no-crypto kullanıldığında, --echo-server veya --echo-client ile sağlanan parola yok sayılır.

- Nping openSSL desteği olmadan derlenmişse bu seçenek belirtilmelidir. Teknik nedenlerden dolayı, --echo-client veya --echo-server bayraklarından sonra, yok sayılacak olsa bile, bir parola sağlanması gerektiğini unutmayın.
- Genel bir Echo sunucusu kurarken --no-crypto bayrağı yararlı olabilir, çünkü kullanıcıların herhangi bir parola veya paylaşılan sır gerekmeden Echo sunucusuna bağlanmasına izin verir. Ancak, kesinlikle gerekli olmadıkça --no-crypto kullanılmaması şiddetle tavsiye edilir. Genel Yankı sunucuları "public" parolasını veya boş parolayı (--echo-server "") kullanacak şekilde yapılandırılmalıdır, çünkü kriptografi kullanımı yalnızca gizlilik ve kimlik doğrulama sağlamakla kalmaz, aynı zamanda mesaj bütünlüğü de sağlar.

`--once` (Serve one client and quit) ⇒ Bu seçenek, Echo sunucusundan bir istemciye hizmet verdikten sonra çıkmasını ister. Bu, sunucuyu kapatmak için uzak ana bilgisayara erişme ihtiyacını ortadan kaldırdığı için yalnızca tek bir Echo oturumu kurulmak istendiğinde kullanışlıdır.

`--safe-payloads` (Zero application data before echoing a packet) ⇒ Bu seçenek, Echo sunucusundan, istemci paketlerinde bulunan uygulama katmanı verilerini yankılamadan önce silmesini ister. Seçenek etkinleştirildiğinde, Echo sunucusu Echo istemcilerinden aldığı paketleri ayrıştırır ve bunların aktarım katmanının ötesinde veri içerip içermediğini belirlemeye çalışır. Böyle bir veri bulunursa, paketler ilgili Yankı istemcisine iletilmeden önce üzerine sıfır yazılır.

- Yankı sunucuları, paralel olarak birden fazla yankı oturumu çalıştıran birden fazla eşzamanlı istemciyi idare edebilir. Hangi paketin hangi istemciye ve hangi oturum üzerinden yankılanması gerektiğini belirlemek için Yankı sunucusu sezgisel bir algoritma kullanır. Bir istemcinin kendi üretmediği bir yankılanan paketi almasını önlemek için aklımıza gelen her türlü güvenlik önlemini almış olsak da, algoritmamızın hata yapma ve bir paketi yanlış istemciye gönderme riski her zaman vardır. safe-payloads seçeneği, bu tür bir hatanın göze alınamayacağı genel yankı sunucuları veya kritik dağıtımlar için kullanışlıdır.

Aşağıdaki örnekler Nping'in Echo modunun ara cihazları keşfetmek için nasıl kullanılabileceğini göstermektedir.

Örnek 18.2. NAT cihazlarını keşfetme

```
# nping --echo-client "public" echo.nmap.org --udp

Starting Nping ( https://nmap.org/nping )
SENT (1.0970s) UDP 10.1.20.128:53 > 178.79.165.17:40125 ttl=64 id=32523 iplen=28
CAPT (1.1270s) UDP 80.38.10.21:45657 > 178.79.165.17:40125 ttl=54 id=32523 iplen=28
RCVD (1.1570s) ICMP 178.79.165.17 > 10.1.20.128 Port unreachable (type=3/code=3) ttl=49 id=16619 iplen=56
[...]
SENT (5.1020s) UDP 10.1.20.128:53 > 178.79.165.17:40125 ttl=64 id=32523 iplen=28
CAPT (5.1335s) UDP 80.38.10.21:45657 > 178.79.165.17:40125 ttl=54 id=32523 iplen=28
RCVD (5.1600s) ICMP 178.79.165.17 > 10.1.20.128 Port unreachable (type=3/code=3) ttl=49 id=16623 iplen=56

Max rtt: 60.628ms | Min rtt: 58.378ms | Avg rtt: 59.389ms
Raw packets sent: 5 (140B) | Rcvd: 5 (280B) | Lost: 0 (0.00%)| Echoed: 5 (140B)
Tx time: 4.00459s | Tx bytes/s: 34.96 | Tx pkts/s: 1.25
Rx time: 5.00629s | Rx bytes/s: 55.93 | Rx pkts/s: 1.00
Nping done: 1 IP address pinged in 6.18 seconds
```

Çıktı, istemcinin yerel ağında bir NAT cihazının varlığını açıkça göstermektedir. Yakalanan paketin (CAPT) gönderilen paketten nasıl farklı olduğuna dikkat edin: orijinal paketlerin kaynak adresi ayrılmış 10.0.0.0/8 aralığındayken, sunucu tarafından görülen adres NAT cihazının İnternet tarafı adresi olan 80.38.10.21'dir. Kaynak port da cihaz tarafından değiştirilmiştir. RCVD ile başlayan satır, Echo sunucusunun çalıştırıldığı makinenin TCP/IP yığını tarafından oluşturulan yanıtlara karşılık gelir.

Örnek 18.3. Şeffaf bir proxy keşfetme

```
# nping --echo-client "public" echo.nmap.org --tcp -p80

Starting Nping ( https://nmap.org/nping )
SENT (1.2160s) TCP 10.0.1.77:41659 > 178.79.165.17:80 S ttl=64 id=3317 iplen=40  seq=567704200 win=1480
RCVD (1.2180s) TCP 178.79.165.17:80 > 10.0.1.77:41659 SA ttl=128 id=13177 iplen=44  seq=3647106954 win=16384 <mss 1460>
SENT (2.2150s) TCP 10.0.1.77:41659 > 178.79.165.17:80 S ttl=64 id=3317 iplen=40  seq=567704200 win=1480
SENT (3.2180s) TCP 10.0.1.77:41659 > 178.79.165.17:80 S ttl=64 id=3317 iplen=40  seq=567704200 win=1480
SENT (4.2190s) TCP 10.0.1.77:41659 > 178.79.165.17:80 S ttl=64 id=3317 iplen=40  seq=567704200 win=1480
SENT (5.2200s) TCP 10.0.1.77:41659 > 178.79.165.17:80 S ttl=64 id=3317 iplen=40  seq=567704200 win=1480

Max rtt: 2.062ms | Min rtt: 2.062ms | Avg rtt: 2.062ms
Raw packets sent: 5 (200B) | Rcvd: 1 (46B) | Lost: 4 (80.00%)| Echoed: 0 (0B)
Tx time: 4.00504s | Tx bytes/s: 49.94 | Tx pkts/s: 1.25
Rx time: 5.00618s | Rx bytes/s: 9.19 | Rx pkts/s: 0.20
Nping done: 1 IP address pinged in 6.39 seconds
```

Bu örnekte, çıktı biraz daha karmaşıktır. Hata mesajlarının olmaması, Echo istemcisinin sunucu ile başarılı bir şekilde Echo oturumu kurduğunu gösterir. Ancak, çıktıda hiçbir CAPT paketi görülemez. Bu, iletilen paketlerin hiçbirinin sunucuya ulaşmadığı anlamına gelir. İlginç bir şekilde, ilk TCP-SYN paketine yanıt olarak bir TCP SYN-ACK paketi alınmıştır (ve ayrıca, hedef ana bilgisayarın 80

numaralı bağlantı noktasının açık olmadığı bilinmektedir). Bu davranış, şeffaf bir web proxy önbellek sunucusunun (bu durumda eski bir MS ISA sunucusu) varlığını ortaya koymaktadır.

Timing and Performance Options (Zamanlama ve Performans Seçenekleri)

`--delay` `<time>` (Delay between probes) ⇒ This option lets you control for how long will Nping wait before sending the next probe. Like in many other ping tools, the default delay is one second. <time> must be a positive integer or floating point number. By default it is specified in seconds, however you can give an explicit unit by appending ms for milliseconds, s for seconds, m for minutes, or h for hours (e.g. 2.5s, 45m, 2h).

`--rate` `<rate>` (Send probes at a given rate) ⇒ Bu seçenek Nping'in saniyede göndermesi gereken prob sayısını belirtir. Bu seçenek ve --delay tersidir; --rate 20, --delay 0.05 ile aynıdır. Her iki seçenek de kullanılırsa, yalnızca parametre listesindeki son seçenek sayılır.

Miscellaneous Options (Çeşitli Seçenekler)

`-h`, `--help` (Display help) ⇒ Yardım bilgilerini görüntüler ve çıkar.

`-V`, `--version` (Display version) ⇒ Programın sürüm numarasını görüntüler ve çıkar.

`-c` `<rounds>`, `--count` `<rounds>` (Stop after a given number of rounds) ⇒ Bu seçenek Nping'in hedef ana bilgisayarlar (ve bazı durumlarda hedef portlar) üzerinde kaç kez döngü yapması gerektiğini belirtmenizi sağlar. Nping bunları "tur" olarak adlandırır. Yalnızca bir hedefin (ve TCP/UDP modlarında yalnızca bir hedef portun) olduğu temel bir yürütmede, tur sayısı hedef ana bilgisayara gönderilen sonda sayısıyla eşleşir. Bununla birlikte, Nping'in birden fazla hedefe ve birden fazla bağlantı noktasına karşı çalıştırıldığı daha karmaşık yürütmelerde, tur sayısı Nping'in tüm hedef IP'leri ve tüm hedef bağlantı noktalarını kapsayan eksiksiz bir prob kümesini gönderme sayısıdır. Örneğin, Nping'den 192.168.1.0-255 ana

bilgisayarlarına ve 80 ve 433 bağlantı noktalarına TCP SYN paketleri göndermesi istenirse, bir turda 256 × 2 = 512 paket gönderilir. Dolayısıyla -c 100 belirtirseniz, Nping farklı hedef ana bilgisayarlar ve bağlantı noktaları üzerinde 100 kez döngü yaparak toplam 256 × 2 × 100 = 51200 paket gönderir. Varsayılan olarak Nping 5 tur boyunca çalışır. Eğer 0 değeri belirtilirse, Nping sürekli olarak çalışacaktır.

`-e` *`<name>`*, `--interface` *`<name>`* (Set the network interface to be used) ⇒ Bu seçenek Nping'e paket göndermek ve almak için hangi arayüzün kullanılması gerektiğini söyler. Nping bunu otomatik olarak algılayabilmelidir, ancak algılayamazsa size söyleyecektir. <name> atanmış bir IP adresi olan mevcut bir ağ arayüzünün adı olmalıdır.

`--privileged` (Assume that the user is fully privileged) ⇒ Nping'e, ham soket gönderimleri, paket koklama ve genellikle özel ayrıcalıklar gerektiren benzer işlemleri gerçekleştirmek için yeterince ayrıcalıklı olduğunu varsaymasını söyler. Varsayılan olarak Nping, root veya yönetici ayrıcalıklarına sahip olmayan bir kullanıcı tarafından bu tür işlemler talep edilirse çıkar. Bu seçenek Linux, BSD veya ayrıcalıksız kullanıcıların ham paket iletimi yapmasına izin verecek şekilde yapılandırılabilen benzer sistemlerde yararlı olabilir. NPING_PRIVILEGED ortam değişkeni --privileged kullanımına alternatif olarak ayarlanabilir.

`--unprivileged` (Assume that the user lacks raw socket privileges) ⇒ Bu seçenek --privileged seçeneğinin tersidir. Nping'e kullanıcıya ağ ham soketi ve koklama ayrıcalıkları yokmuş gibi davranmasını söyler. Bu, test, hata ayıklama veya işletim sisteminizin ham ağ işlevselliği bir şekilde bozulduğunda kullanışlıdır. NPING_UNPRIVILEGED ortam değişkeni --unprivileged kullanımına alternatif olarak ayarlanabilir.

`--send-eth` (Use raw ethernet sending) ⇒ Nping'in paketleri daha yüksek IP (ağ) katmanı yerine ham ethernet (veri bağlantısı) katmanında göndermesini ister. Nping varsayılan olarak, üzerinde çalıştığı platform için genellikle en iyi olanı seçer. Ham soketler (IP katmanı) genellikle Unix makineler için en verimlisiyken, Microsoft ham soket desteğini devre dışı bıraktığından beri Windows çalışması için ethernet çerçeveleri gereklidir. Nping, bu seçeneğe rağmen başka seçenek olmadığında (ethernet olmayan bağlantılar gibi) hala ham IP paketlerini kullanır.

`--send-ip` (Send at raw IP level) ⇒ Nping'in daha düşük seviyeli ethernet çerçeveleri göndermek yerine ham IP soketleri üzerinden paket göndermesini ister. Bu --send-eth seçeneğinin tamamlayıcısıdır.

`--bpf-filter` `<filter spec>` `--filter` `<filter spec>` (Set custom BPF filter) ⇒ Bu seçenek özel bir BPF filtresi kullanmanızı sağlar. Varsayılan olarak Nping, gönderilen belirli problara verilen en yaygın yanıtları yakalamayı amaçlayan bir filtre seçer. Örneğin, TCP paketleri gönderilirken filtre, hedef portu probun kaynak portuyla eşleşen paketleri veya probun bir sonucu olarak hedef veya herhangi bir ara cihaz tarafından oluşturulabilecek ICMP hata mesajlarını yakalayacak şekilde ayarlanır. Herhangi bir nedenle gönderilen sondalara yanıt olarak garip paketler bekliyorsanız veya yalnızca belirli bir trafik türünü koklamak istiyorsanız, tcpdump gibi araçlar tarafından kullanılan BPF sözdizimini kullanarak özel bir filtre belirleyebilirsiniz. Daha fazla bilgi için http://www.tcpdump.org/ adresindeki belgelere bakın.

`-H`, `--hide-sent` (Do not display sent packets) ⇒ Bu seçenek Nping'e gönderilen paketler hakkında bilgi yazdırmamasını söyler. Bu, çok kısa problar arası gecikmeler kullanıldığında (yani, flood yaparken) yararlı olabilir, çünkü standart çıktıya bilgi yazdırmanın bir hesaplama maliyeti vardır ve bunu devre dışı bırakmak muhtemelen işleri biraz hızlandırabilir. Ayrıca, aktif ana bilgisayarları veya açık portları tespit etmek için Nping kullanırken yararlı olabilir (örneğin, bir /24 alt ağındaki tüm TCP portlarına prob göndermek). Bu durumda, kullanıcılar gönderilen binlerce probu değil, yalnızca aktif ana bilgisayarlar tarafından oluşturulan yanıtları görmek isteyebilir.

`-N`, `--no-capture` (Do not attempt to capture replies) ⇒ Bu seçenek Nping'e paket yakalamayı atlamasını söyler. Bu, gönderilen problara yanıt olarak gelen paketlerin işlenmeyeceği veya görüntülenmeyeceği anlamına gelir. Bu, taşma ve ağ yığını stres testleri yaparken faydalı olabilir. Bu seçenek belirtildiğinde, yürütmenin sonunda gösterilen istatistiklerin çoğunun işe yaramayacağını unutmayın. Bu seçenek TCP Connect modunda çalışmaz.

Output Options (Çıktı Seçenekleri)

`-v[` `<level>` `]`, `--verbose [` `<level>` `]` (Increase or set verbosity level) ⇒ Verbosity seviyesini artırarak Nping'in çalışması sırasında daha fazla bilgi yazdırmasına neden olur. 9 verbosity seviyesi vardır (-4 ila 4). Her -v örneği ayrıntı düzeyini bir artırır (varsayılan değer olan 0 düzeyinden). Her -q seçeneği örneği ayrıntı düzeyini bir azaltır. Alternatif olarak -v3 veya -v-1'de olduğu gibi seviyeyi

doğrudan belirtebilirsiniz. Bunlar mevcut seviyelerdir:
Level -4 ⇒ Hiç çıktı yok. Bazı durumlarda Nping'in herhangi bir çıktı üretmesini istemeyebilirsiniz (iş arkadaşlarınızdan birinin omzunuzun üzerinden sizi izlemesi gibi). Bu durumda seviye -4 yararlı olabilir, çünkü herhangi bir yanıt paketi görmeseniz de, problar gönderilmeye devam edecektir.

Level -3 ⇒ Seviye -4 gibi ancak ölümcül hata mesajlarını görüntüler, böylece Nping'in çalışıp çalışmadığını veya bir hata nedeniyle başarısız olup olmadığını gerçekten görebilirsiniz.

Level -2 ⇒ Seviye -3 gibi ancak uyarıları ve kurtarılabilir hataları da görüntüler.

Level -1 ⇒ Geleneksel çalışma zamanı bilgilerini (sürüm, başlangıç zamanı, istatistikler, vb.) görüntüler ancak gönderilen veya alınan paketleri göstermez.

Level 0 ⇒ Bu varsayılan ayrıntı düzeyidir. Seviye -1 gibi davranır ancak gönderilen ve alınan paketleri ve diğer bazı önemli bilgileri de görüntüler.

Level 1 ⇒ Seviye 0 gibi ancak zamanlama, bayraklar, protokol ayrıntıları vb. hakkında ayrıntılı bilgi görüntüler.

Level 2 ⇒ Seviye 1 gibi ancak gönderilen ve alınan paketler ve diğer ilginç bilgiler hakkında çok ayrıntılı bilgiler görüntüler.

Level 3 ⇒ Seviye 2 gibi ancak gönderilen ve alınan paketlerin ham onaltılık dökümünü de görüntüler.

Seviye 4 ve üstü ⇒ Seviye 3 ile aynı.

`-q[ <level> ]`, `--reduce-verbosity [ <level> ]` (Decrease verbosity level) ⇒ Verbosity seviyesini düşürerek Nping'in çalışması sırasında daha az bilgi yazdırmasına neden olur.

`-d[ <level> ]` (Increase or set debugging level) ⇒ Verbose modu bile sizin için yeterli veri sağlamadığında, hata ayıklama sizi çok daha fazlasıyla doldurmak için kullanılabilir! v'de olduğu gibi, hata ayıklama bir komut satırı bayrağı olan -d ile etkinleştirilir ve hata ayıklama seviyesi birden fazla kez belirtilerek artırılabilir. 7 hata ayıklama seviyesi vardır (0 ila 6). Her -d örneği hata ayıklama seviyesini bir artırır. Seviyeyi doğrudan ayarlamak için -d'ye bir argüman sağlayın; örneğin -d4.

Hata ayıklama çıktısı, Nping'de bir hatadan şüphelendiğinizde veya Nping'in ne yaptığı ve neden yaptığı konusunda kafanız karıştığında kullanışlıdır. Bu özellik çoğunlukla geliştiriciler için tasarlandığından, hata ayıklama satırları her zaman

açıklayıcı değildir. Şöyle bir şeyle karşılaşabilirsiniz

```
NSOCK (1.0000s) Callback: TIMER SUCCESS for EID 12; tcpconnect_event_handler(): Received callback of type TIMER with status SUCCESS
```

Bir satırı anlamadıysanız, tek çareniz onu görmezden gelmek, kaynak koduna bakmak veya geliştirme listesinden (nmap-dev) yardım istemektir. Bazı satırlar kendi kendini açıklar, ancak hata ayıklama seviyesi arttıkça mesajlar daha belirsiz hale gelir. Bunlar mevcut seviyelerdir:

Level 0 ⇒ Seviye 0. Hiç hata ayıklama bilgisi yok. Bu varsayılan düzeydir.

Level 1 ⇒ Bu seviyede, yalnızca çok önemli veya üst düzey hata ayıklama bilgileri yazdırılacaktır.

Level 2 ⇒ Seviye 1 gibi ancak önemli veya orta düzey hata ayıklama bilgilerini de görüntüler

Level 3 ⇒ Seviye 2 gibi ancak normal ve düşük seviyeli hata ayıklama bilgilerini de görüntüler.

Level 4 ⇒ Seviye 3 gibi ama aynı zamanda sadece gerçek bir Nping manyağının görmek isteyeceği mesajları görüntüler.

Level 5 ⇒ Seviye 4 gibi ancak Nsock gibi harici kütüphanelerle ilgili temel hata ayıklama bilgilerini etkinleştirir.

Level 6 ⇒ Seviye 5 gibi, ancak Nsock gibi harici kütüphanelerle ilgili tam, çok ayrıntılı hata ayıklama bilgileri sağlar.

Bugs (Hatalar)

Yazarları gibi, Nping de mükemmel değildir. Ancak hata raporları göndererek ve hatta yamalar yazarak daha iyi olmasına yardımcı olabilirsiniz. Nping beklediğiniz gibi davranmazsa, önce https://nmap.org adresinden erişilebilen en son sürüme yükseltin. Sorun devam ederse, daha önce keşfedilmiş ve ele alınmış olup olmadığını belirlemek için biraz araştırma yapın. Çok sayıda forumu bir araya getirdiği için sorunu veya hata mesajını Google'da aramayı deneyin. Bundan bir şey çıkmazsa, izleyicimizde bir Sorun oluşturun (http://issues.nmap.org) ve/veya dev@nmap.org adresine bir hata raporu gönderin. Göndermeden önce nmap-dev

listesine abone olursanız, mesajınız moderasyonu atlayacak ve daha hızlı ulaşacaktır. https://nmap.org/mailman/listinfo/dev adresinden abone olun. Lütfen sorun hakkında öğrendiğiniz her şeyi, kullandığınız Nping sürümünü ve hangi işletim sistemi sürümünde çalıştığını da ekleyin. Nping'i geliştirmek için diğer öneriler de Nmap dev posta listesine gönderilebilir.

Nping'i geliştiren veya bir hatayı düzelten bir yama yazabiliyorsanız, bu daha da iyi! Yama veya git çekme isteği göndermek için talimatlara https://github.com/nmap/nmap/blob/master/CONTRIBUTING.md adresinden ulaşabilirsiniz.

Güvenlik raporları gibi özellikle hassas konular doğrudan Fyodor'a fyodor@nmap.org adresinden gönderilebilir. Diğer tüm raporlar ve yorumlar bunun yerine geliştirici listesini veya sorun izleyiciyi kullanmalıdır, çünkü daha fazla kişi bunları okur, takip eder ve yanıtlar.

Authors (Yazarlar)

Luis MartinGarcia `<luis.mgarc@gmail.com>` (`http://www.luismg.com`)

Fyodor `<fyodor@nmap.org>` (`https://insecure.org`)

A. Nmap XML Output DTD (A. Nmap XML Çıktı DTD)

Purpose (Amacı)

Bu belge türü tanımı (DTD) XML ayrıştırıcılar tarafından Nmap XML çıktısını doğrulamak için kullanılır. En son sürüm her zaman https://svn.nmap.org/nmap/docs/nmap.dtd adresinde mevcuttur. Öncelikle programatik kullanım için tasarlanmış olsa da, insanların Nmap XML çıktısını yorumlamasına yardımcı olma değeri nedeniyle buraya dahil edilmiştir. DTD, formatın yasal öğelerini tanımlar ve genellikle alabilecekleri nitelikleri ve değerleri sıralar. DTD'nin kullanımı "XML Çıktısı (-oX)" başlıklı bölümde daha ayrıntılı olarak ele alınmaktadır.

The Full DTD (Tam DTD)

https://nmap.org/book/nmap-dtd.html

Index

https://nmap.org/book/idx.html