

NMAP Network Güvenlik Tarayıcısı Kullanım Klavuzu

Lisans

Bu döküman **Fatih Özavcı** tarafından **NMAP**'in İngilizce yazılmış "manual" sayfasından derlenmiştir. Anlatımı kolaylaştırmak amacıyla bazı bölümler çıkartılmış bazı yerler ise değiştirilmiştir. Yazarın ve Derleyeninin haklarına saygı duyarak her türlü kaynaktan yazılması ve yayınlanması serbesttir.

NMAP Network Güvenlik Tarayıcısı Kullanım Klavuzu

Nmap, sistem yöneticilerinin geniş ağlarını taramasında ve hangi istemci/sunucusunda hangi servislerin çalıştığını saptamasında kullanılabileceği bir araç olarak tasarlandı. Nmap geniş bir tarama yelpazesini destekler ; UDP, TCP Connect, TCP SYN (Yarı Açık), FTP Proxy Bounce Atağı, TCP FIN, TCP Xmass Tree, ICMP (Ping Sweep), ACK Sweep, SYN Sweep ve Null Scan bunlara birkaç örnektir. Bahsi geçen port türleriyle ilgili daha ayrıntılı bilgi bu yazının ilerleyen bölümlerinde ve *Port Tarama Nedir?* yazımızda bulunmaktadır. Nmap ayrıca gelişmiş özelliklere sahip bir araçtır, TCP/IP parmak izleri ile hedefin işletim sistemini saptayabilir, Stealth (Gizli) tarama yapabilir, taramalarında dinamik zamanlamalar kullanılabilir, paralel taramalar yapabilir, ping atarak aktif hostları bulabilir, RPC taraması yapabilir, esnek port ve hedef özelliklerine sahiptir. Unutulmaması gereken en önemli nokta hedef sistemde açık olan portların nmap'in standart olarak nitelendirilen ve /etc/services dosyasından aldığı port numarası ve sunucu servis karşılaştırılmaları tablosu aracılığıyla tespit edilmiş olmasıdır. Örnek olarak standart kullanımda 21/TCP ftp protokolü için kullanılan bir port olması dolayısıyla bu portu açık bulan nmap servisin ftp olduğunu bildirecektir, ancak o portu dinleyen servis farklı bir servis (örneğin vnc sunucusu) olabilir. Şimdi neler yapabileceği anlatıldığına göre sıra bunların nasıl yapıldığını anlatmaya geldi.

Tarama Türleri

-sT TCP Connect Scan : En basit anlamda çalışan tarama tekniğidir, hedef porta bağlanmak için SYN paket gönderir, karşılığında SYN/ACK paketi gelirse ACK paketi göndererek porta bağlanır ve portun açık olduğunu rapor eder, eğer SYN paketine RST cevabı gelirse portun kapalı olduğunu rapor eder. Bu tarama türünde extra paket özelliklerine sahip olmak gerekmediği için root olmayan kullanıcılarda kullanılabilir. En kötü özelliği açılan tüm oturumların hedef sistem, Firewall yada IDS tarafından loglanıyor olmasıdır.

-sS TCP SYN Scan : Yarı açık olarak tanınan SYN tarama oturumu tamamen açmaz, SYN paketinin karşılığında SYN/ACK paketi geldiğinde portun açık olduğunu rapor eder ve RST paketi göndererek oturumu kapatır, port kapalı ise hedef zaten direk RST cevabı gönderir. Bu yöntemi uygulayabilmek için root olmak gerekmektedir. IDS ve Firewall'lara yakalanma ihtimali ve loglanma ihtimali azdır.

-sF, -sX, -sN : Bu tarama yöntemleri ise sırayla gizli FIN , Xmass Tree ve Null Scan'dir. IDS ve Firewall'ların SYN taramaları loglayabileceğini düşünerek kullanılan yöntemlerdir. FIN, Xmass Tree ve Null scan paketlerinin gönderilmesi durumunda hedefin RFC 793'te açıklandığı gibi kapalı olan tüm portlar için RST cevabı göndermesi mantığına dayanır. Bu yöntem IPeye ve NmapNT ile windows platformunda da uygulanabilmektedir. Ayrıca bu tarama yöntemleri açık port buluyorsa (FIN taramada Windows sistemlerindeki tüm portlar açık olarak görünmektedir, çünkü Windows tabanlı sistemler bir oturuma ait olmayan FIN paketleri ile karşılaşılırsa tümünü göz ardı ederler ve göz ardı edilen paketler standart olarak portun açık olduğu anlamına gelir.) hedefin sistemi Windows tabanlı değildir. Eğer SYN scan açık port buluyor ve bu tarama yöntemleri bulamıyor ise hedef Windows tabanlı bir sisteme sahip demektir. Nmap'in İşletim sistemi saptama özelliklerine bu durum dahildir. Windows'la aynı tepkiyi veren bazı sistemler ise Cisco, BSDI, HP/UX, MVS ve IRIX' tir.

-sP Ping Sweep : Taranılan ağda hangi hostların aktif olduğuna ihtiyaç olduğunda kullanılan genel yöntem ICMP Echo paketleri gönderip cevap beklemektir, son zamanlarda bu ping isteklerinin Firewall'lar tarafından bloke edildiği düşünüldüğünde alternatif çözümler geliştirilmelidir. Bu durumda nmap TCP ACK paketi gönderiyor (standart olarak 80. porttan - değiştirilebilir), eğer porttan RST cevabı geliyorsa sistemin aktif olduğu rapor ediliyor. Diğer alternatif teknikle bir SYN paket gönderip hedeften SYN/ACK yada RST cevabı beklemektir, her iki cevapta sistemin aktif olduğunu gösterir. Root olmayan kullanıcılar için ise standart TCP Connect yöntemi kullanılır. Standart olarak ICMP ve ACK teknikleri paralel olarak uygulanır. Eğer bunun değiştirilmesi istenirse -P* parametreleri kullanılarak bu yöntemler değiştirilebilir. Ayrıca bu pingleme işlemi tamamlandığında sadece aktif sistemler taranır, bu seçenek ping taraması kullanmadan port taramaya geçmek isteniyorsa kullanılabilir.

-sU UDP Scan : Bu teknik hedef bilgisayarın UDP portlarından hangilerinin açık olduğunu saptamak için kullanılır. (RFC 768) Hedef makinede açık olduğu düşünülen porta 0 byte'lik bir UDP paket göndermek ve "ICMP Port Unreachable" paketini beklemek temeline dayanır. Paket gelirse port kapalı gelmezse açık olduğuna karar verilir. Bazı insanlar UDP taramayı önemsemeyizler. Önemsemelerini gerektiren sebepler arasında Tftp, NFS, Snmp gibi protokollerin UDP üzerinden çalışması ve Solaris'in RPCbind açığı sayılabilir.

-sA ACK Scan : ACK tarama yöntemi Firewall'ların ACL'lerini bypass ederek tarama yapılmasını sağlar. Bazı Firewall'lar stateful yada basit paket filtreleme Firewall'ları olabilir, dışarıdan gelen SYN paketlerini bloke edebilir ancak ACK flag'lı paketin geçişine izin veriyor olabilir. Rastgele üretilmiş ack/sequence numaralarıyla yapılır. Cevap gelmezse yada ICMP port unreachable mesajı geliyorsa port filtrelenen bir porttur. Nmap genellikle portlar için unfiltered nitelmesi yapmaz. Bu taramada bulunan portları asla açıkca 'open' olarak nitelendirmez.

-sW Window Scan : Bu gelişmiş tarama türü ACK tarama türüne çok benzer, portların açık olup olmadığını taraması dışında bu portları filtered/unfiltered olarak nitelendirir ve çerçeve boyutundaki farklılıklardan hedefin işletim sistemini saptar. Aralarında AIX, Amiga, BeOS, BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital UNIX, FreeBSD, HP-UX, OS/2, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.X, Ultrix, VAX ve VxWorks gibi işletim sistemlerinde bulunduğu işletim sistemlerinin bazı versiyonları bu durumdan etkilenir. Tam listeye ulaşabilmek için Nmap-Hackers posta listesinin arşivlerine bakılabilir.

-sR RPC Scan : RPC taramaları için diğer tarama türleriyle beraber kullanılır. Bütün TCP/UDP portları tarayarak açık bulunduğu portlarda SunRPC'nin "NULL" komutlarını kullanarak rpc portlarını saptamaya çalışır, eğer rpc portu bulursa çalışan program ve sürümlerini saptamaya çalışır. Böylece Firewall yada diğer paket filtreleme cihazları hakkında bazı işe yarar bilgiler saptamaya çalışır. Decoy özelliği şu an için RPC taramalarda kullanılmıyor ancak bazı UDP RPC taramalarında bu özellik nmap'e eklenmiştir.

-b (ftp relay host) : Ftp protokolünün ilginç bir özelliği proxy için destek vermesidir (RFC 959). Bunun için öncelikle hedefin ftp sunucusuna bağlanmak gereklidir, daha sonra internette herhangi bir yerden o sunucuya bir dosya gönderilebilir. RFC'nin yazıldığı 1985 yılından günümüze kadar ftp bu özelliğe sahip olabilir. Böylece bir ftp sunucusu üzerinden TCP port tarama yapabilme imkânında kazanılmış olur. Bu seçenek ile bu denemeler uygulanabilir.

Genel Seçenekler

-P0 : Ping atmayı denemeden tüm hostları nmap'e taratmak için kullanılır. Bazı ağlar ICMP Echo ve ICMP Echo Reply paketlerini bloke etmektedir, böyle durumlarda -P0 yada -PT80 kullanılmalıdır. Böylece Firewall'un arkasındaki sistemleri saptama imkânı kazanılmaktadır.

-PT : TCP ping atılarak aktif sistemlerin saptanması için kullanılmaktadır. ICMP Echo paketlerinin engellendiği ağlarda TCP ACK flag'lı paketler göndererek etkili olmaktadır. Eğer hedef sistemler aktif ise RST flag'lı paketler gönderir ve böylece aktif olduğu anlaşılır. Bu seçeneğin kullanılması için root olunması gereklidir. -PT[port] şeklinde kullanılır, varsayılan portu 80'dir. Eğer hedef ağda kullanılan filtreleme cihazı statik paket filtreleme cihazı ise bu paketin erişim kontrol listelerine rağmen içeri girmesi mümkündür.

-PS : SYN flag'lı paketler ile TCP ping taraması için kullanılır. Hedefe SYN flag'lı bir paket gönderilir ve hedeften RST yada SYN/ACK flag'lı paketler beklenir. Eğer bu paketlerden biri gelirse hedefin aktif olduğuna karar verir.

-PI : Standart ICMP ping taramaları için kullanılır. Hedefe ICMP Echo (type 0) paketi göndererek karşılığında ICMP (type 8) paketi bekler, eğer bu paket gelirse hedefin aktif olduğuna karar verir. Ayrıca bu tarama türüyle broadcast ping'de atılmaktadır ve böylece broadcast ping isteklerine cevap veren bilgisayarlarda saptanmaktadır. Bu durum hedefe denial of service (servis durdurma) saldırılarından bazılarını test etmek içinde kullanılır. (Smurf, TFN gibi)

-PB : Varsayılan ping taramalarında kullanılacak ping türüdür. 2 yönlü olarak yapılmaktadır. İlki ACK (-PT) flag'lı TCP paketiyle ikincisi ise ICMP Echo paketleriyle yapılan ping türüdür. Firewall'ların arkasındaki sistemleri belirlemek için ikisinden sadece biri kullanılır.

-O : Bu seçenek aktif durumdaki hedef sistemin TCP/IP parmakizleriyle işletim sistemini saptamak için kullanılır. Taratılan hedefin işletim sistemini tüm taramalardaki farklılıkları birleştirerek saptamaktadır. Bu taramalara işletim sistemlerinin verdikleri cevaplar nmap tarafından bir veritabanında tutulmaktadır ve karşılaştırmalar bu veritabanı üzerinden yapılmaktadır. Bu veritabanında düzenlemeler yaparak bilinen işletim sistemlerinin listeye eklenmesi mümkündür. Eğer nmap tanımadığı bir işletim sistemi olduğunu söylüyorsa ve siz bu işletim sisteminin hangi işletim sistemi olduğu ve versiyonu hakkında bilgiye sahipseniz nmap'in yazarı Fyodor'un fyodor@dhp.com adresine mail yolu ile çıktıları gönderebilirsiniz. Daha ayrıntılı bilgi almak için *Nmap'in Anasayfasında* bulunan "Remote OS detection via TCP/IP Stack FingerPrinting" isimli dökümana başvurabilirsiniz. Bu dökümanın *Egemen Taş tarafından çevrilmiş türkçe sürümünde* mevcuttur.

-I : Bu seçenek Ident protokolü ile tarama yapma imkânı sunmaktadır. Dave Goldsmith tarafından 1996 yılında Bugtraq posta listesine atılan postada Ident protokolünün (RFC 1413) herhangi bir servisi başlatan kullanıcının saptanmasına izin verdiği belirtilmiştir. Örneğin eğer http portu açık ise ve dinleyen servisi başlatan kullanıcının root olduğu saptanıyorsa bu programdan kaynaklanabilecek olası güvenlik zayıflıkları işletim sistemine root haklarıyla erişimi sağlayabilir. Diğer tarama yöntemleri ile beraber kullanılır ancak hedef bilgisayarda Identd aktif durumda değil ise kullanılabilir durumda değildir.

-f : Bu seçenek SYN, FIN , XMAS veya Null taramalarda kullanılabilir durumdadır. Teori hedef sistemdeki Firewall , diğer paket filtreleme cihazlarının yada saldırı tespit sistemlerinin parçalanmış paketlerden taramayı farkedemeyecekleri temeline dayanmaktadır. Kullanılması tavsiye edilmektedir. Ancak bu teknik hedef sistemlerde gelen parçalar bekletilip bütün parçalar geldikten sonra hedefe gönderiyorsa işe yarayamaz. Bu özellik henüz tüm işletim sistemleri üzerinde çalışmamaktadır ; ancak Linux , FreeBSD ve OpenBSD üzerinde çalışmaktadır. Diğer *nix sistemlerde başarı ile çalıştırılması durumunda yazara bildirilmesi rica edilmektedir.

-v : Verbose seçeneğinin kullanımı tavsiye edilmektedir çünkü taramalar hakkında daha fazla bilgi gösterilmesini sağlamaktadır. Çıktıları iki kez alma imkanı böylece kavuşulmuş olur, eğer bu çıktılar yetmiyorsa -d seçeneği ile ekrana tamamen sığamayacak kadar bilgi alınabilir.

-h : Nmap'in sıkça kullanılan bazı parametrelerinin kullanımı konusunda yardımcı bilgiler içerir. Bir nevi hızlı başvuru klavuzu denilebilir.

-oN (Log Dosyası) : Nmap'in ürettiği sonuçları ismi verilen dosyaya yazmasını sağlar.

-oM (Log Dosyası) : Nmap'in ürettiği sonuçları ismi verilen dosyaya makine okuyabilir şekilde yazmasını sağlar. / | , gibi noktalama işaretleriyle sonuçları ayırır. -v parametresi kullanılarak daha fazla ayrıntı yazdırılması da sağlanabilir.

--resume (Log Dosyası) : CTRL+C ile yarıda kesilen taramaların devam etmesi için kullanılır. Ancak yarıda kesilen tarama -oN yada -oM kullanılarak bir log dosyasına kayıt edilmiş olmalı ve bu log dosyası parametre ile verilmelidir. Nmap bu log dosyasındaki başarılı son taramadan itibaren taramaya devam eder.

-iL (Log Dosyası) : Nmap'e taranacak hedeflerin bir dosya aracılığıyla verilmesini sağlar. Bu dosyada hedefler boşluk , sekme yada yeni satırlarla sıralanmış olabilir.

-p (port aralığı) : Bu seçenek ile nmap'in özel port aralıklarını taraması sağlanabilir. Örneğin -p 23 hedefin 23. portunu tarayacaktır. -p 20-30, 139, 60000-` ise 20 ile 30 arasındaki tüm portların 139. portun ve 60000'den büyük tüm portların taranmasını sağlayacaktır. Varsayılan değeri 1 ile 1024 arasındaki tüm portlar ve /etc/services dosyasında listelenmiş portların taranmasıdır.

-F Hızlı tarama : Özel bir portun taranması istenmiyorsa , sadece /etc/services dosyasındaki portların taranması isteniyorsa kullanılacak bir seçenektir.

-D [yanıltma1], [yanıltma2], [ME] : Hedefi tararken ait olduğu sistemin IP'sini saklamaya yardımcı olur. Normalde taramalar bir IDS , Firewall yada diğer paket filtreleme cihazlarına kaydedilebilir ve gelen paketler bu sistemden geldiği için IP bilgisi log dosyalarına kaydedilmektedir. Ancak decoy yani yanıltma yada tuzak kullanıldığı durumda bu sistemin IP si ile beraber parametre olarak verilen diğer IP'lerde taramalarda görünecektir ve onlardan da hedefe paket geliyormuş gibi olacaktır. Bu durum bazı paket filtreleme cihazlarının ve port tarama saptayıcılarının yanıltılmasına veya birden fazla hata vermesine sebep olabilmektedir, böylece söz konusu tarama çok daha az dikkat çekecektir. Yanıltmalar aralarında ` , ` işaretleri ile ayrılarak girilmelidir, istenirse parametrelere `ME` seçeneği eklenerek bu sistemin IP'sinin de decoyler arasında istenilen sırada bulunması sağlanabilir. Bazı port tarama saptayıcılar (Örneğin scanlogd) 6. pozisyon yada sonrasında bu sistemin IP'sini farkedemeyebilir. Eğer `ME` seçeneği yanıltmalar arasında kullanılmazsa nmap sistem IP'sini rastgele bir pozisyona koyacaktır. Dikkat edilmesi gereken bir durumda seçilen yanıltmaların aktif durumda olması yada kazayla hedefe SYN Flood denilen DOS atağının yapılma olasılığıdır. Ayrıca kullanılan yanıltmaların tamamının aktif olmaması durumunda kolayca port taramayı yapan sistem anlaşılacaktır. Yanıltma özelliği ping taramalarında da (ICMP, SYN , ACK yada hangisi olursa) kullanılabilir durumdadır. Yanıltma ayrıca -O seçeneği yani işletim sistemi saptama seçeneği ile beraber kullanılabilir. Kullanılan yanıltmaların sayısı kadar taramalarda yavaşlayacaktır. Ayrıca bazı ISP'ler spoof yapılmış yani yanıltılmış IP'lerin barındığı paketleri hedefe ulaşmadan önce kendi ağ bölümünden olmadığı için engelleyebilir.

-S (IP Adresi) : Bazı durumlarda nmap sistemin kaynak IP'sini belirleyemeyecektir, ki burada söyleyecektir. Böyle durumlarda -S seçeneğini kullanarak kaynak IP'si nmap'e belirtilebilir. Ayrıca bu seçenek ile IP spoofing denilen adres yanıltmasında kullanılabilir. Örneğin taramalarda hedefin rakip şirketinin IP'leri kullanılabilir, bu epey yanıltıcı olacaktır. Ancak bu seçeneğin böyle kullanılması desteklenmemektedir. Çünkü bu durum taramalardan başkalarının sorumlu tutulma ihtimalini yükseltmektedir. -e seçeneği genellikle bu seçenek kullanılırken gerekli olmaktadır.

-e (arayüz) : Nmap'e taramaları yaparken paketleri hangi ağ arayüzünü kullanarak gönderebileceğinin belirtilmesini sağlar. Nmap bunu bazı durumlarda belirleyemekte ve bunu söylemektedir.

-g (port numarası) : Taramalarda paketlerin kaynak portlarını isteklere göre belirlemeyi sağlar. Bazı paket filtreleme cihazları ve Firewall'lar oturumun ilk olarak hangi taraftan başlatıldığını saptayamayabilirler. Genelde statik paket filtreleme cihazlarında karşılaşılan bir durum olmasına rağmen dinamik paket filtreleme cihazlarında da benzer durumlar geçerlidir. Böylece 20/TCP ftp data ve 53/TCP-UDP gibi portların kaynak port olarak ayarlanması durumunda filtreleme cihazlarının erişim kontrol listelerinin içinden geçerek hedefe ulaşma gibi bir şans sunulur. Genelde saldırganlar gönderdikleri paketlerde kaynak portları bu şekilde ayarlayarak paketlerini ftp yada dns geri dönüşleriymiş gibi maskeleyebilir ve filtreleme cihazlarını geçme şansı kazanırlar. UDP taramalarında 53/UDP, TCP taramalarında ise 53/TCP'den önce 20/TCP yani FTP-DATA portu kullanılabilir. Nmap -g seçeneği ile kaynak portu belirleme şansını sunmaktadır.

-r : Nmap'e taramalarda portları rastgele değilde sırayla taramasını belirtmek için kullanılır.

--randomize_hosts : Nmap'in verilen aralıktaki taranacak sistemleri rastgele sırayla taramasını sağlamak için kullanılır. Bazı IDS'lere yakalanmamak için bu teknik ile beraber işlemleri zamanlama seçeneklerini kullanarak yavaşlatmakta etkili olabilir.

-M (en fazla soket sayısı) : Aynı anda açılacak en fazla soket sayısını belirtmek için kullanılır. Taramaları daha yavaş yaparak yakalanmamak ve hedef sistemin çökmesini engellemek için kullanılabilir.

Zamanlama Seçenekleri

Genellikle Nmap ağ yapılarına göre zamanlamasını ve daha hızlı/yavaş tarama şekillerini belirleyebilir, böylece saptanamayan sistem sayısını minimuma indirmiş olur. Ancak nmap'in zamanlama ayarlarında değişiklik yapma ihtiyacı olduğunda aşağıdaki parametreler kullanılarak bu değerlerin değiştirilmesi mümkündür.

-T (Paranoid | Sneaky | Polite | Normal | Aggressive | Insane) : Bu seçenek belirli zaman periyotlarının ve belirli son bekleme sürelerinin poliçelere aktarılmış halidir ve kullanımı kolaylaştırmak için yapılmıştır. Paranoid , taramalar yavaşça ve aralarında fazlaca zaman bırakarak IDS'lere yakalanmadan taramanın tamamlanması için yapılmıştır. Sneaky, taramalar arası 15 sn. aralıklarla paketleri gönderir. Polite, hedef ağı kolayca meşgul edebilecek ve hedef sistemi kilitleyebilecek kadar hızlı bir taramadır. Portların taranması arasında 0.4 sn. den az bir zaman vardır. Normal, standart nmap tarama süreleridir. Aggressive, sistem başına 5 dakikalık bekleme süresi ve 1.25 sn.lik bir porttan cevap bekleme süresine sahiptir. Insane, hızlı ağlarda kullanışlıdır, sistem başına 0.75 sn.lik bekleme port başına ise 0.3 sn. cevap bekleme süresine sahiptir. Bu arada seçenek içinde poliçenin sadece adını yazmak yerine sayısını yazılabilir, -T0 Paranoid -T5 ise Insane'e karşılık gelmektedir.

--host_timeout (milisaniye) : Bir sistemin taranması durumunda özel bekleme süresinin belirlenmesi için kullanılır. Standart olarak nmap süre sınırı belirtmez.

--max_rtt_timeout (milisaniye) : Nmap'in bir porta gönderdiği paketin cevabını bekleyeceği sürenin en fazla ne kadar olacağını belirlenmesi için kullanılır, standart değerin 9000 olduğu varsayılır.

--min_rtt_timeout (milisaniye) : Nmap sistemin cevaplarının çabuk gelmesi durumunda bekleme süresinin değerini düşürmektedir. Böyle durumlarla karşılaşmamak ve belirli bir bekleme süresini garantiye almak amacıyla verilebilecek en az bekleme süresidir. Böylece zaman farkından kaynaklanacak paket kayıpları minimuma indirilmiştir olur.

--initial_rtt_timeout (milisaniye) : İlk araştırma için süre sınırı belirtmeyi sağlar. Genellikle sadece Firewall ile korunan sistemlerin -P0 seçeneği ile taranması durumunda kullanışlıdır. Normalde nmap ilk ping isteği ve ilk birkaç denemeden sonra iyi bir rtt zamanlaması yapar. Varsayılan değeri 6000'dir.

--max_parallelism (sayı) : Aynı anda en fazla kaç işlemin beraber yapılabileceğinin belirlenmesi için kullanılır. Bu seçenek ayrıca RPC taraması , Ping taraması gibi taramaları etkiler.

--scan_delay (milisaniye) : Taranan portlar arasındaki bekleme zamanının belirlenmesini sağlar. Ağı fazla yüklememek, hedef sistemi kilitlememek ve sessizce tarayarak IDS'lere yakalanmamak için kullanışlıdır.

Hedef Özellikleri

Nmap oldukça esnek bir hedef seçme özelliğine sahiptir. İstenirse IP adresi vererek /maske ile taranacak ağı belirtmek mümkündür. Örneğin /24 C sınıfı bir ağ için /16 B sınıfı bir ağ için kullanılabilir. Ayrıca B sınıfı bir ağı taramak için 128.210.*.* , `128.210.*.*` , 128.210.0-255.0-255 yada 128.210.0/16 gibi düzenler kullanılabilir. Bu tanımlamaların hepsi geçerlidir.

Örnekler

```
nmap -v -sS -O www.ornek.com
```

Bu örnekte -v seçeneği daha fazla bilgi almayı , -sS seçeneği SYN tarama uygulanmasını , -O seçeneği ise hedefin işletim sistemini saptamayı sağlar.

```
nmap -sX -p 22,53,110,143,4564 128.210.*.1-127
```

Bu örnekte ise -sX seçeneği Xmass Tree taramasının uygulanmasını , 22,53,110,143,4564 nolu portların taranmasını ve 128.210.*.1-127, 128.210.0/16 ağında IP'si 1 ile 127 arasındaki tüm hostların taranmasını ifade eder.