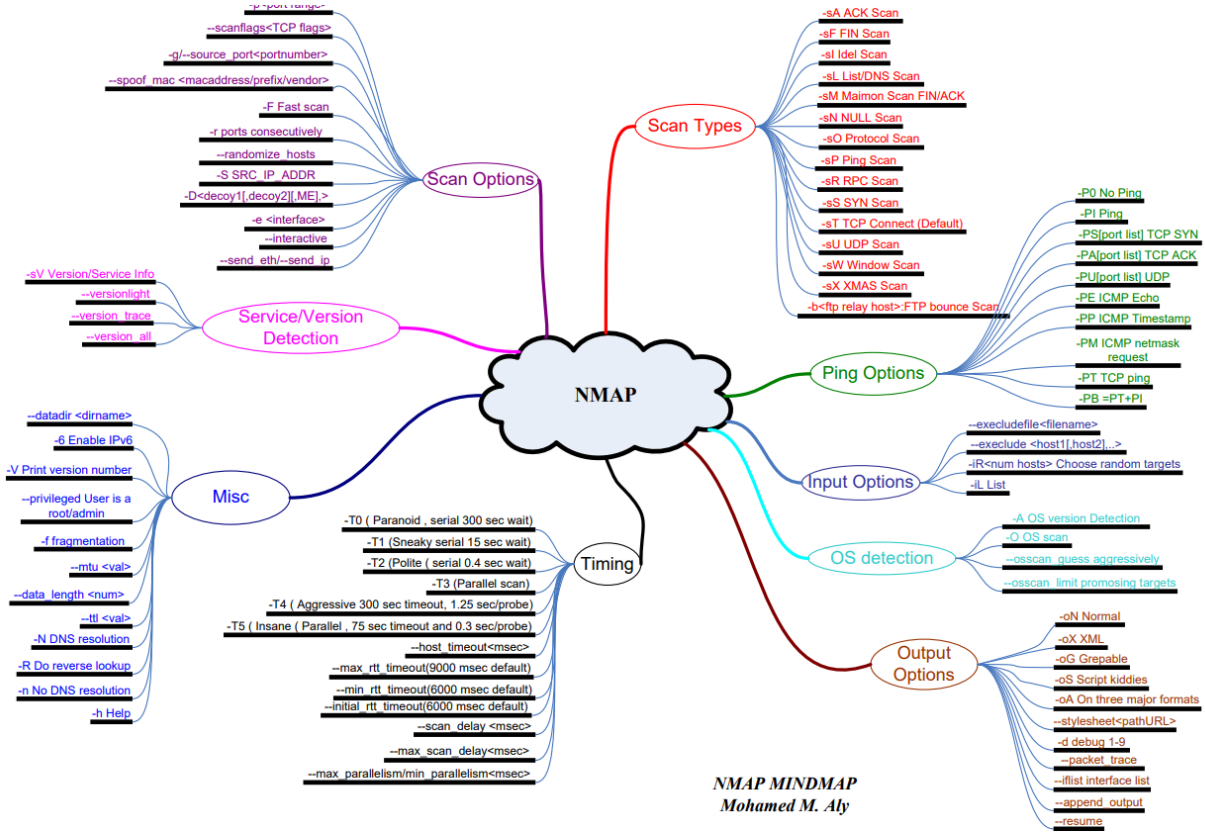
Nmap - UDP and host/service discovery

Hakan Duran

UDP servislerini taramak



DNS, SNMP ve DHCP (registered ports 53, 161/162, and 67/68) en çok kullanılan UDP portlarıdır. UDP taraması TCP taramasına göre daha yavaş olduğu için genelde UDP taraması güvenlikçiler tarafından es geçilebilmektedir.

UDP taraması -sU parametresi ile gerçekleştirilmektedir. Aynı portta hem UDP hem TCP taraması yapılabilmesi için -sS (SYN taraması) gibi parametreler eklenebilir.

UDP taraması hedef porta UDP paketi gönderilerek yapılır. Çoğu port için, paket boş olacaktır (payload'sız). Nmap, bazı popüler portlara spesifik payload'a sahip paketler gönderebilir.

Karşı tarafın cevabı	Nmap'in değerlendirmesi
Hedef porttan UDP cevabı (nadir)	open
Cevap alınamazsa (tekrar denemelerden sonra bile) :	open|filtered
"ICMP port unreachable" hatası (type 3, code 3)	closed

Diğer ICMP unreachable hataları (type 3, code 1, 2, 9, 10, or 13)	filtered

En çok merak edilen değerlendirme, open|filtered değerlendirmesidir. UDP taramalarında karşı taraf bir cevap iletmek zorunda değildir. Nmap, yaygın portlara spesifik payload'lara sahip UDP paketleri göndererek cevap alabilmeyi amaçlar. Port halihazırda kullanımda olsa bile, payload'ı olmayan bir pakete cevap vermemeyi tercih edebilir (genel davranış), port sadece dinliyor ve cevap vermiyor şeklinde tasarlanmış olabilir, veya firewall porta gelen UDP isteklerini discard ediyor olabilir. Bu gibi birçok nedenden ötürü cevap gelmemesi halinde open|filtered denmektedir.

Bir başka problemse taramanın uzun sürmesidir. 1000 portu taramak yaklaşık 17 dakika almaktadır. Bunun sebeplerinden birisi de çoğu Linux sistemlerinde ICMP cevap hızı sınırlamasıdır.

Filtered ile open portları birbirinden ayırmak

UDP servisleri genelde Nmap'ın boş veya spesifik payload'a sahip paketlerinden farklı UDP paketleri kabul etmektedir. Her yaygın UDP servisine cevap alınabilir bir paket yollamak için büyük bir database'e ihtiyaç vardır. Nmap bu amaç için nmap-service-probes biçiminde bu veritabanına sahiptir. Bu veritabanı Chapter 7, *Service and Application Version Detection* kısmında anlatılmıştır.

Versiyon tarama -sV (veya -A) ile olanak tanındığında, Nmap, her open|filtered ve open porta UDP paketleri gönderecektir. Eğer bu paketler sayesinde bir dönüt alınabilirse open|filtered port open'a dönecektir. Versiyon tarama kullanmak, bazı open|filtered portların open olduğunu garantilese de, 1000 port taramak yaklaşık 1 saat alabilir.

Nmap tarafından önerilen bir yöntem açık olduğu tahmin edilen TCP veya UDP portlarına Nmap veya Nping gibi araçlar kullanarak traceroute uygulamaktır.

Bir başka yöntem ise yaygın portlar için uygulamaya özel araçlar denemektir. Bir SNMP portuna brute-force paketler göndererek cevap almaya çalışmak örnek olabilir. Nmap'in versiyon tespit etmek için kullandığı database gün geçtikçe büyüdüğünden bu tarz saldırılara olan ihtiyaç azalmaktadır.

UDP taramasını hızlandırmak

Open ve filtered portlar nadiren cevap göndermektedir, bu durum Nmap'in tekrar UDP paketi gönderip tekrar test etmesine sebebiyet vermektedir. Closed portlar ise esasen daha sıkıntılı olabilmektedir. Bunun nedeni, işletim sistemlerinin "ICMP port unreachable" paketlerini limitlemesinden kaynaklanmaktadır. Linux ve Solaris'in bu konuda katı bir politikaya sahip olduğu söylenebilir. Nmap'in sitesindeki bir örnekte Linux 2.4.20, 1 saniyede 1 "ICMP port unreachable" paketine izin vermektedir. Bu politika Linux kernelinin net/ipv4/icmp.c kısmında tanımlanmıştır. Linux'un bu limiti 65536 portun taramasını 18 saatten uzun hale getirmektedir.

Nmap'in taramayı hızlandırmak için bazı önerileri aşağıda listelenmiştir:

- Aynanda birçok host taranabilir. --min-hostgroup parametresi ile ayarlanabilir.
- Önce yaygın portları taramak işi hızlandıracaktır. -F parametresi ile ayarlanabilir.
- Versiyon tespitinin dahil edildiği taramalara --version-intensity 0 eklenebilir. Versiyon tespiti (-sV), open ve filtered portları ayırmada kullanılır. Ancak versiyon tespiti taramayı önemli ölçüde

azaltır. Bunun nedeni, versiyon tespitinde her porta uygulamaya spesifik payload'a sahip birçok paket gönderilmesidir. --version-intensity 0 Nmap'i belirtilen porta sadece en olası payload'ları yollar. Bunu nmap-service-probes dosyasını kullanarak yapar.

- Firewall'ın arkasından tarama yapın. Firewall'ların paket filtrelemeleri taramayı yavaşlatan bir etmendir. Firewall'ı bypass etme yolu bulunmuşsa bu durum kullanılarak tarama yapılabilir. Örneğin, firewall bir port üzerinden ağ içi cihazlarla iletişimimize olanak vermişse, o port üzerinden kapsüllenmiş paketler yollamak ve daha sonra ağ içinde açmak; veya ağ içindeki bir cihaza taramayı yaptırmak örnek gösterilebilir.
- --host-timeout parametresi kullanılarak yavaş cevap veren hostlarda tarama askıya alınabilir.

Örnek karşılaştırma

Aşağıdaki karşılaştırma aynı host'a -sUV parametreleri ile tarama yapmaktadır. İlki 1 saat sürerken, ikincisi 13 saniye sürmüştür.

```
krad# nmap -sUV -T4 scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT   STATE SERVICE VERSION
53/udp open  domain  ISC BIND 9.3.4

Nmap done: 1 IP address (1 host up) scanned in 3691.89 seconds
----------------------
krad# nmap -sUV -T4 -F --version-intensity 0 scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 99 open|filtered ports
PORT   STATE SERVICE VERSION
53/udp open  domain  ISC BIND 9.3.4

Nmap done: 1 IP address (1 host up) scanned in 12.92 seconds
```

Host bulma

Host keşif ihtiyaçları çok çeşitli olduğundan Nmap, kullanılan teknikleri özelleştirmek için çok çeşitli seçenekler sunar. Ping taraması ismine rağmen, bu, her yerde bulunan ping aracıyla ilişkili basit ICMP yankı isteği paketlerinin çok ötesine geçer. Kullanıcılar, bir liste taramasıyla (-sL) veya ping'i devre dışı bırakarak (-Pn) ping adımını tamamen atlayabilir veya çok bağlantı noktalı TCP SYN/ACK, UDP ve ICMP araştırmalarının isteğe bağlı kombinasyonlarıyla ağa bağlanabilir. Birçok ağda, herhangi bir zamanda IP adreslerinin yalnızca küçük bir yüzdesi etkindir. Bu özellikle 10.0.0.0/8 gibi özel adres alanlarında yaygındır. Bu ağda 16,8 milyon IP bulunuyor ancak Nmap, bunun binden az makineye sahip şirketler tarafından kullanıldığını gördüklerini söylüyor.

Host bulma aşamasında Nmap, reverse DNS uygulayabilmektedir. Bunu önlemek için parametre -n (No DNS resolution)'dir. -R parametresi belirtilen tüm IP'lere reverse DNS yapar. Default olan sadece cevap veren host'lara reverse DNS yapılmasıdır.

-sL opsiyonu sadece belirtilenen IP aralığına DNS reverse işlemi ugulamaktadır. IP'lere herhangi bir paket yollamamaktadır. Bunu yapmaktaki amaç daha baştan IDS'lere yakalanmamaktır. DNS reverse işlemi hedef IP aralığından bağımsız olduğu için IDS'lere yakalanma olasılığı çok düşüktür.

```
felix~> nmap -sL www.stanford.edu/28

Starting Nmap ( https://nmap.org )
Host www9.Stanford.EDU (171.67.16.80) not scanned
Host www10.Stanford.EDU (171.67.16.81) not scanned
Host scriptorium.Stanford.EDU (171.67.16.82) not scanned
.
.
Host leland2.Stanford.EDU (171.67.16.93) not scanned
Host coursework-j.Stanford.EDU (171.67.16.94) not scanned
Host 171.67.16.95 not scanned
Nmap done: 16 IP addresses (0 hosts up) scanned in 0.38 seconds
```

-sn parametresi Nmap'a host keşfinden sonra port taraması yapmaması gerektiğini söyler. Kaç host'un aktif olduğu -sL'de verilen listeden genelde daha önemlidir. -sn parametresi bir "ICMP echo request", 443. porta TCP SYN paketi, 80. porta TCP ACK paketi ve bir "ICMP timestamp request" gönderir.

-Pn "disable ping" anlamına gelir ve host keşfini tamamen atlar. -Pn parametresi, Nmap'in belirtilen tüm IP adreslerine verilen tüm taramaları yapacağı anlamına gelir. Bunu yapmanın nedenlerinden birisi host keşfini kısıtlayan firewall olabileceği şüphesidir. Bu durumda host var mı yok mu diye kontrol edilmeden port taraması gerçekleştirilebilir. -Pn parametresini kullanmada bir başka neden host keşfinin gereksiz olabileceğidir. Nmap'e -iL parametresi kullanarak taraması yapılacak IP adresleri verilir ve host taraması yapılmaz. Nmap'e göre bunu yapmak gereksizdir, çünkü eğer hostlardan en az biri bile aktif değilse bu büyük bir zaman kaybına yol açacaktır. Ayrıca Nmap, host keşfi sırasında elde ettiği RTT örneklerini port taramasını hızlandırma amacıyla kullanabilmektedir.

Host keşfi yöntemleri

Host keşfinde birçok yöntem vardır. TCP SYN Ping (-PS<port list>), TCP ACK Ping (-PA<port list>), UDP Ping (-PU<port list>), ICMP Ping Types (-PE, -PP, and -PM), IP Protocol Ping (-PO<protocol list>) ve ARP Scan (-PR) bunlara örnektir.

-PU<port list> bu raporu ilgilendiren kısımdır. Belirtilen portlara UDP paketi gönderir. Eğer herhangi bir port belirtilmemişse default 40125. porttur. Port taramasında olduğu gibi eğer yaygın portlar belirtilirse (53 gibi) Nmap, payload'a sahip UDP paketleri göndererek host'un varlığını araştırabilir.

Eğer gönderilen UDP paketinin ardından gelen cevap "ICMP port unreachable" ise bu closed anlamına gelir ve karşı tarafın aktif ve ulaşılabilir olduğunu, sadece o porttan yayın yapılmadığını gösterir. Diğer tarz ICMP hata paketleri (örn. host/network unreachable veya TTL exceeded) ise host'un down veya

ulaşılamaz olduğunu gösterir. Cevabın olmaması da burada down olarak değerlendirilmektedir ancak host cevap vermemeyi de seçmiş olabilir. -PU parametresinin asıl kullanım amacı firewall bypass olabilir. Bazı cihazlar tüm TCP portlarını bloke ederek görünmemeye çalışabilirler ancak UDP servislerine aynı şekilde bloke edilmezse buradan bir host'un varlığı anlaşılabilir.

--data-length <*length*>

Bu parametre gönderilecek olan pakete payload yükler. Yukarıda bazı örneklerde payload'sız paket gönderimi gerçekleşmektedir. Rastgele length byte data payload olur. Bazı IDS'ler (Snort da dahil olmak üzere), payload'sız ping paketlerine karşı alert oluşturmaktadır. Bu parametre ile evasion gerçekleştirilebilir. 32 değeri paketi Windows'tan, 56 değeri ise Linux'tan geliyormuş gibi benzetebilir.