

# NMAP

Nmap, sızma testlerinde ve zaafiyet bulmak için yapılan taramalarda yaygın olarak kullanılan bir yazılımdır. Yerel ağı, uzaktaki bir bilgisayarın veya bir web sitesininin ağ bilgilerini denetlemek ve keşfetmek için kullanılabilir.

- Tam bir bilgisayar ağ haritası oluşturur.
- Ana bilgisayarların uzak IP adreslerini bulur.
- Taradığınız ağdaki bilgisayarların işletim sistemlerini ve yazılım ayrıntılarını görüntüler.
- Yerel veya uzaktaki ağlarda açık portları algılayabilir.
- Kendi bilgisayarınızı veya aınızı taratarak güvenlik açıklarınızı görmeyi ve onları fark edip düzeltmenize olanak sağlar.

## Port nedir?

Portlar, bilgisayarlar arasında veri iletişimi sağlayan fiziksel veya sanal bağlantı noktalarını ifade eder. Bu bağlantı noktaları, ağ üzerindeki cihazların belirli uygulamalar veya servisler arasında veri alışverişi yapabilmesini mümkün kılar.

Her bir port, bir sayı ile temsil edilir

**Port 21 (FTP - File Transfer Protocol):**

**FTP portu, dosya transferi için kullanılır. Bu port açıksa, dosya transferi amacıyla FTP istemcileri veya sunucuları arasında iletişim kurulabilir.**

**Port 22 (SSH - Secure Shell):**

**SSH portu, güvenli uzak erişim ve dosya transferi için kullanılır. Açık bir SSH portu üzerinden uzaktaki bir bilgisayara güvenli bir şekilde bağlanabilirsiniz.**

**Port 23 (Telnet):**

**Telnet portu, uzaktaki bir bilgisayara terminal erişimi sağlar.**

**Port 25 (SMTP - Simple Mail Transfer Protocol):**

**SMTP portu, e-posta gönderimi için kullanılır. Açık bir SMTP portu üzerinden e-posta sunucularına erişim sağlanabilir.**

**Port 53 (DNS - Domain Name System):**

**DNS portu, alan adlarını IP adreslerine çevirmek için kullanılır. Açık bir DNS portu, DNS sorgularının yapılmasını sağlar.**

**Port 80 (HTTP - HyperText Transfer Protocol):**

**HTTP portu, web tarayıcıları ve web sunucuları arasındaki standart iletişim portudur. Bu port açıksa, web sayfalarına erişim mümkündür.**

**Port 110 (POP3 - Post Office Protocol 3):**

**POP3 portu, e-posta alımı için kullanılır. E-posta istemcileri, bu portu kullanarak e-postalarını indirebilirler.**

**Port 143 (IMAP - Internet Message Access Protocol):**

**IMAP portu, e-posta sunucuları ile e-posta istemcileri arasında iletişim kurmak için kullanılır. E-posta kutularındaki mesajlara erişim sağlar.**

**Port 443 (HTTPS - HyperText Transfer Protocol Secure):**

**HTTPS portu, web tarayıcıları ve güvenli web sunucuları arasındaki iletişim için kullanılır. Bu port, SSL/TLS şifreleme protokollerini kullanarak güvenli bir bağlantı sağlar.**

**Port 135 (RPC - Remote Procedure Call):**

Windows işletim sistemlerinde kullanılan bir porttur. RPC servisleri, uzak bilgisayarlarla iletişim kurmak için kullanılır. Açık olması durumunda, RPC üzerinden sistem bilgileri alınabilir veya sistem üzerinde bazı işlemler gerçekleştirilebilir.

#### **Port 194:**

Belirli bir servise veya uygulamaya atanan özel bir porttur. Açık olması durumunda, kullanılan uygulama belirlenmelidir.

#### **Port 445 (Microsoft-DS - Microsoft Directory Services):**

Windows işletim sistemlerinde dosya ve yazıcı paylaşımı için kullanılır. Açık olması durumunda, bu port üzerinden dosya sistemine erişim sağlanabilir.

#### **Port 1433 (Microsoft SQL Server):**

Microsoft SQL Server veritabanı hizmeti tarafından kullanılır. Açık olması durumunda, SQL Server'a erişim sağlanabilir ve veritabanı ile etkileşimde bulunulabilir.

#### **Port 3306 (MySQL):**

MySQL veritabanı sistemine erişim sağlamak için kullanılır. Açık olması durumunda, MySQL veritabanına bağlanabilir ve sorgular gerçekleştirilebilir.

#### **Port 3389 (RDP - Remote Desktop Protocol):**

Uzak masaüstü bağlantıları için kullanılır. Açık olması durumunda, uzaktaki bir bilgisayara RDP üzerinden bağlantı kurulabilir.

## **TCP (Transmission Control Protocol)**

Internet üzerindeki veri iletişimi için yaygın olarak kullanılan bir taşıma protokolüdür. TCP segmentleri, bilgisayarlar arasındaki güvenilir veri iletişimini sağlamak için kullanılır. Bu segmentlerin başlıkları, çeşitli kontrol bayraklarını içerir. İşte TCP başlıklarındaki bazı önemli kontrol bayrakları ve işlevleri:

#### **URG (Urgent):**

Bu bayrak, "acil" durumu belirtir. Eğer URG bayrağı set edilmişse, TCP segmenti içindeki belirli verilerin öncelikli olduğunu gösterir. Ancak, modern uygulamalarda genellikle kullanılmaz.

#### **ACK (Acknowledgment):**

ACK bayrağı, alınan bir veri paketinin onaylandığını gösterir. Bu bayrak, veri alındığında karşı tarafın bunu onaylaması için kullanılır.

#### **PSH (Push):**

PSH bayrağı, alıcıya veriyi hemen işlemesi gerektiğini bildirir. Bu bayrak, alınan verinin tamamının üst katman uygulamasına hızlı bir şekilde teslim edilmesini sağlar.

#### **RST (Reset):**

RST bayrağı, bir bağlantıyı sıfırlamak veya aniden sonlandırmak için kullanılır. RST gönderen taraf, karşı tarafın durumunu sıfırlar ve bir hata veya kapatma durumu olabilir.

#### **SYN (Synchronize):**

SYN bayrağı, bir bağlantı kurma isteğini başlatır. İki taraf arasında bir TCP üç yönlü el sıkışma sürecinde kullanılır. Bağlantı kurmak isteyen taraf SYN gönderir, karşı taraf ise bu SYN'i alır ve kendi SYN'ini gönderir.

#### **FIN (Finish):**

FIN bayrağı, bir bağlantının kapatılması için kullanılır. İki taraf arasında bir bağlantının sonlandırılmasını belirtir. Gönderen taraf, FIN bayrağını göndererek bağlantıyı sonlandırma isteğini ifade eder.

Bu bayraklar, TCP protokolü üzerindeki iletişim süreçlerini kontrol etmek ve yönlendirmek için kullanılır. İki cihaz arasındaki TCP bağlantısının başlatılması, veri alışverişi ve sonlandırılması gibi işlemler, bu bayraklar aracılığıyla gerçekleştirilir. TCP'nin güvenilir bir iletişim protokolü olmasının temelinde, bu tür kontrol bayraklarının etkili kullanımı yatar.

## **Three-Way Handshake**

Bilgisayarlar arasında güvenilir bir TCP bağlantısı kurmak için kullanılan bir protokol adım dizisidir. Bu adım dizisi, veri iletimi için güvenilir bir kanal oluşturur ve her iki tarafın birbirlerini tanımasını sağlar. Three-Way Handshake'in temel amacı, TCP bağlantısının başlatılması ve uygun bir şekilde senkronize edilmesidir. Aşağıda Three-Way Handshake adımları açıklanmıştır:

#### **Step 1- SYN (Synchronize):**

Gönderen taraf (Client), bir bağlantı başlatmak istediğini belirten bir TCP segmenti gönderir. Bu segmentin içinde SYN bayrağı (Synchronize) set edilmiştir. Gönderen taraf, kendi başlatıcı bir sayı olan bir Initial Sequence Number (ISN) gönderir. Bu sayı, gönderilen verinin başlangıcını belirtir.

#### **Step 2- SYN-ACK (Synchronize-Acknowledge):**

Alıcı taraf (Server), SYN bayrağı ile karşı tarafın bağlantı kurma isteğini kabul ettiğini ve kendi ISN'sini gönderdiğini belirten bir TCP segmenti ile cevap verir. Alıcı taraf aynı zamanda ACK bayrağını da set eder. Bu aşamada, alıcı tarafın da kendi başlatıcı bir sayısı (ISN) vardır.

#### **Step 3- ACK (Acknowledge):**

Gönderen taraf, alıcı tarafın SYN-ACK'yi aldığını ve bağlantıyı kabul ettiğini doğrulamak için ACK bayrağını set eden bir TCP segmenti gönderir. Bu segmentte, alıcının ISN'sine bir artı eklenerek ACK bayrağı ile birlikte gönderilen sayı, alıcı tarafın iletişimde bulunabileceği bir sonraki byte'ı işaretler.

Bu üç adımlı el sıkışma süreci tamamlandığında hem gönderen taraf hem de alıcı taraf, birbirlerini tanıyan ve güvenli bir iletişim kurmaya hazır bir TCP bağlantısına sahip olurlar. Bu bağlantı üzerinden güvenilir bir veri iletimi gerçekleşebilir. Three-Way Handshake, TCP'nin güvenilir ve düzenli veri iletimini sağlamasına yardımcı olur.

## **Port durumları**

Bir bilgisayar sistemindeki veya ağdaki belirli bir portun açık, kapalı veya dinleme modunda olup olmadığını belirtir. Port durumları, genellikle bir bilgisayarın güvenlik durumunu değerlendirmek ve ağa potansiyel saldırı

noktalarını belirlemek amacıyla kullanılır. İşte yaygın olarak kullanılan port durumları ve anlamları:

#### **Açık (Open):**

Portun açık olması, belirli bir servis veya uygulamanın o porta bağlanmak ve iletişim kurmak için kullanılabileceği anlamına gelir. Açık portlar, potansiyel saldırılara karşı savunmasız olabilir ve güvenlik riski taşıyabilir.

#### **Kapalı (Closed):**

Kapalı bir port, belirli bir servise veya uygulamaya bağlantı izni verilmediği veya bu portun kullanımının devre dışı bırakıldığı anlamına gelir. Kapalı portlar, ağ güvenliği için bir önlem olarak kapatılmış olabilir.

#### **Dinleme (Listening):**

Dinleme modundaki bir port, belirli bir servisin veya uygulamanın bağlantı taleplerini kabul etmeye hazır olduğu anlamına gelir. Dinleme durumundaki bir port, gelen bağlantıları bekleyen bir servisi veya uygulamayı temsil eder.

#### **Filtrelenmiş (Filtered):**

Filtrelenmiş bir port, güvenlik duvarı veya ağ cihazları tarafından engellendiği anlamına gelir. Bu durumda, bağlantı talepleri filtrelenmiş veya engellenmiş olabilir. Filtrelenmiş portlar, ağ güvenliğini artırmak için kullanılır.

#### **Açık | Filtrelenmiş (Open|Filtered):**

Bu durum, belirli bir portun açık olup olmadığını veya filtrelenmiş olduğunu belirtir, ancak belirli bir durumu belirlemek mümkün değildir. Bu durum, port tarama sırasında belirli bir yanıt alınamadığında ortaya çıkabilir.

#### **Kapalı | Filtrelenmiş (Closed|Filtered):**

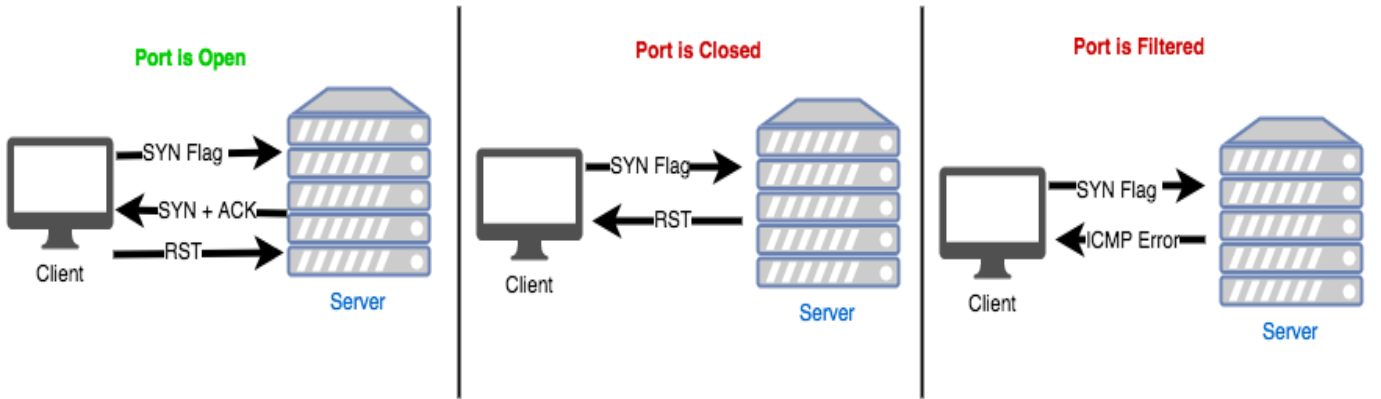
Bu durum, belirli bir portun hem kapalı hem de filtrelenmiş olduğunu belirtir. Bu durumda, portun ne durumda olduğu belirlenememiştir.

Port durumları, güvenlik açısından önemli bir role sahiptir. Açık ve gereksiz portlar, potansiyel güvenlik riskleri oluşturabilir. Güvenlik duvarları ve diğer ağ güvenlik önlemleri, açık portları minimumda tutmak ve gerekli olanları dikkatlice yönetmek için kullanılır. Port durumları, ağ yöneticilerine ve güvenlik uzmanlarına ağlarını daha güvenli hale getirme ve saldırılara karşı koruma sağlama konusunda yardımcı olabilir.

## TCP SYN SCAN

Çok hızlı bir tarama çeşididir. Bu taramayı gerçekleştirmek için admin ya da root olmak gerekir. TCP bağlantısını tam olarak gerçekleştirmediği için nispeten gizli bir taramadır. Çünkü uzaktaki sunucuyla tam teşekküllü bir bağlantı kurmaya çalışmaz. ACK paketi gönderilmez yani 3 yollu el sıkışma tamamlanmaz.

**NOT:** Gizleme işlemi garanti edilmez. Modern paket yakalama programları ve gelişmiş güvenlik duvarları artık TCP SYN taramalarını anlayabiliyorlar.



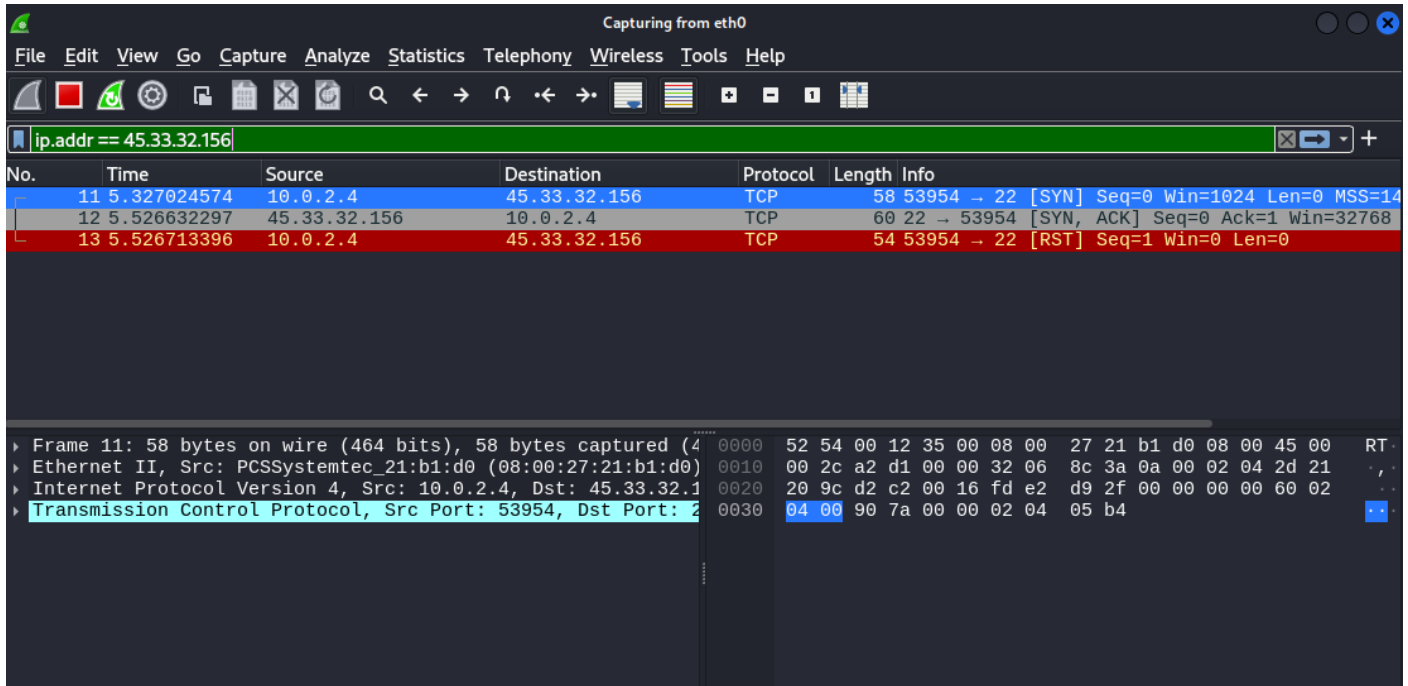
**Port açıksa:** Nmap'in 3 yollu el sıkışmayı tamamlamasına gerek yoktur. Burada RST bayrağı gönderilmezse hedef sürekli SYN/ACK göndermeye devam eder. O yüzden RST paketi gönderilir

**Port kapalıysa:** Burada port kapalı olduğu için sunucu direk RST bayrağı ve ack paketi yollar.

**Port filtrelense:** ilk olarak SYN paketi gönderilir ve yanıt beklenir. Eğer yanıt gelmezse genellikle filtrelili porttur ama kesin değildir. Yani portun açık olup gönderilen paketin düşme ihtimali vardır (ağda kesinti). NMAP yeniden bir

**SYN paketi gönderir ve yine cevap alamazsa filtrelendiğini belirtip devam eder.**

**-sS seçeneği bir TCP SYN taraması yapar. Kullanım Şekli : nmap -sS [hedef]**



No.	Time	Source	Destination	Protocol	Length	Info
11	5.327024574	10.0.2.4	45.33.32.156	TCP	58	53954 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	5.526632297	45.33.32.156	10.0.2.4	TCP	60	22 → 53954 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0
13	5.526713396	10.0.2.4	45.33.32.156	TCP	54	53954 → 22 [RST] Seq=1 Win=0 Len=0

Frame 13: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_21:b1:d0 (08:00:27:21:b1:d0), Dst: 10.0.2.4 (08:00:00:08:00:02)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 45.33.32.156
Transmission Control Protocol, Src Port: 53954, Dst Port: 22, Seq: 53954, Win: 0, Len: 0

## TCP CONNECT SCAN

**Ayrıcalıklı olmayan kullanıcılar için varsayılan tarama türü -sT taramasıdır. IPv6 hedeflerini tararken de kullanılır. TCP Bağlantı Taraması, herhangi bir gizli bilgi kullanmadan uzaktaki sisteme doğrudan bağlanmaya çalışan basit bir bağlantı şeklidir.**

**Sistem bu taramada yarı açık bağlantı gerçekleştirmek yerine tam bağlantı yapar. Bu yüzden hem daha uzun sürer hem de daha fazla paket gerektirir. Ayrıca hedef makine üzerinde log tutulmasına sebep olur. İyi bir IDS taramayı yakalayacaktır.**

**NMAP bağlandıktan hemen sonra hiçbir veri göndermeden bağlantıyı kopardığı zaman sistemindeki bir çok servis hedefteki sistemin loglarına not bırakacaktır.**

**NOT:** Nmap'i mümkün olduğunca root yetkilerle çalıştırmak en iyisidir, çünkü TCP / SYN taramasını (-sS) gerçekleştirir ve bu da port durumlarının daha doğru bir listesini sunabilir ve önemli ölçüde daha hızlıdır



## Port açıksa:

**NMAP 3 yollu el sıkışmayı tamamlar bağlantıyı sağlar ve hedef sistem veri gönderir.**

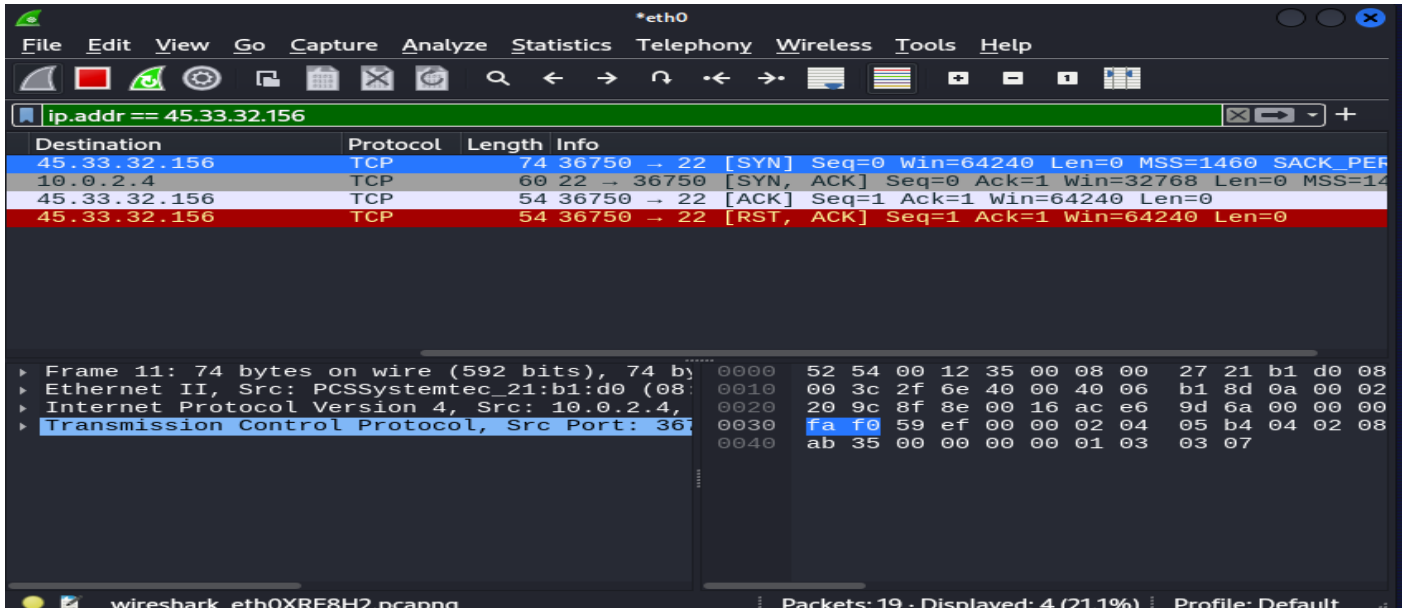
**NMAP hemen bağlantıyı sonlandırır.**

**TCP bağlantıları genelde FIN bayrağı ile sonlandırılır ancak Nmap RST bayrağı ile bağlantıyı hemen koparır.**

**Portun kapalı ve filtreli olması durumunda SYN taraması ile aynı tepkileri verir.**

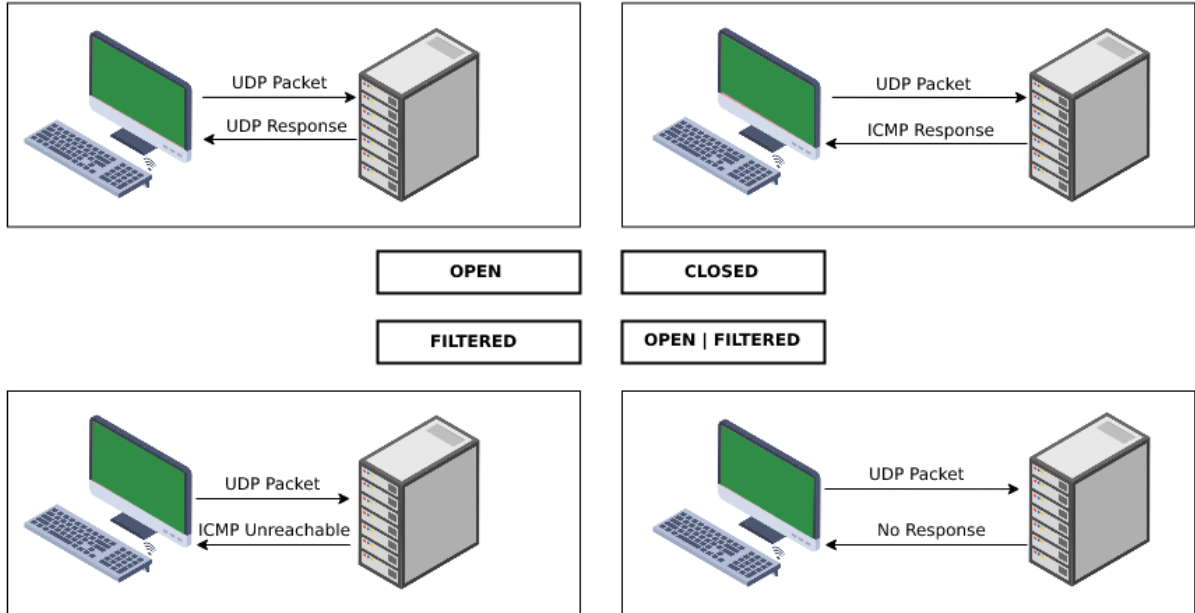
**-sT seçeneği bir TCP bağlantılı tarama gerçekleştirir.**

**Kullanım Şekli: nmap -sT [hedef]**



## UDP SCAN

**TCP en çok kullanılan taşıma katmanı protokolüdür fakat, birçok ağ hizmeti (DNS, DHCP ve SNMP gibi) UDP'yi kullanmaktadır. Bir ağ denetimi gerçekleştirirken, hedef ana bilgisayar / ağın daha kapsamlı bir resmini elde etmek için hem TCP hem de UDP hizmetlerini kontrol etmek gerekir.UDP de TCP gibi bayraklar yoktur.**



**Port açıksa:** UDP taramasında gönderilen UDP paketine karşılık olarak herhangi bir UDP cevabı döner.

**Port kapalıysa:** UDP taramasında gönderilen UDP paketine karşılık olarak ICMP cevabı döner.

**Port açık filtreliyse:** UDP taramasında gönderilen UDP paketine karşılık olarak cevap dönmezse NMAP yeniden bir UDP paketi gönderir. Gönderilen bu UDP paketine de herhangi bir cevap gelmeme durumunda nmap portun durumunu open filtered olarak belirler.

**Port filtreliyse:** UDP taramasında gönderilen UDP paketine karşılık olarak ICMP farklı unreachable error kodları dönerse port filtreli olarak döner.

-sU seçeneği bir UDP (User Datagram Protocol-Kullanıcı Datagram Protokolü) taraması yapar.

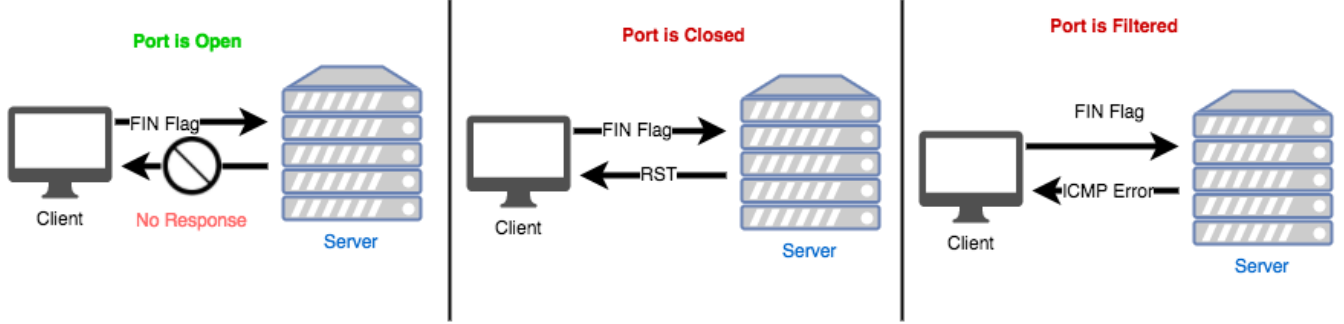
Kullanım Şekli : nmap -sU [hedef]

## FIN SCAN

Nmap bu taramayı gerçekleştirirken hedef porta bir FIN bayrağı gönderir ve hedeften gelen yanıtlara göre portun kapalı ya da açık olduğunu belirler.

-sF seçeneği bir TCP FIN taraması yapar.

Kullanım Şekli : nmap -sF [hedef]



## NULL SCAN

Bir TCP NULL taraması, Nmap'ın TCP bayraklarının etkin olmadığı paketleri göndermesine neden olur. Bu, paket başlığını 0 (sıfır) olarak ayarlayarak yapılır. Bir hedefe NULL paketleri göndermek, bir yanıt üretmek için güvenlik duvarlı bir sistemi kandırmanın bir yöntemidir.

**NOT:** Bazı sistemler bu taramaya cevap vermeyebilir

-sN seçeneği TCP NULL taramasını gerçekleştirir.

Kullanım Şekli : `nmap -sN [hedef]`

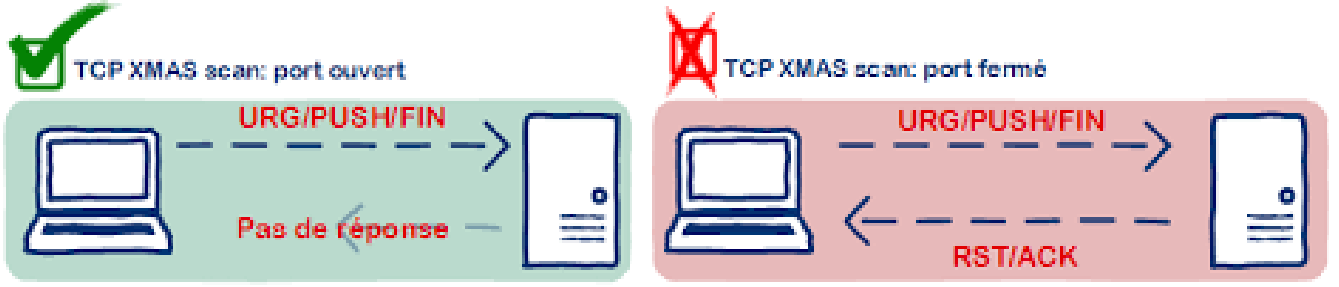


## XMAS SCAN

Xmas taramasında Nmap, URG, FIN ve PSH ile paketleri gönderir ve bayraklar etkinleştirilir. Bu, paketin "yılbaşı ağacı gibi aydınlatılması" etkisine sahiptir ve güvenlik duvarı ile korunan bir sistemden bir yanıt isteyebilir. **NOT:** Bazı sistemler bu taramaya cevap vermeyebilir

**-sX seçeneği bir Xmas taraması yapar.**

**Kullanım Şekli : nmap -sX [hedef]**



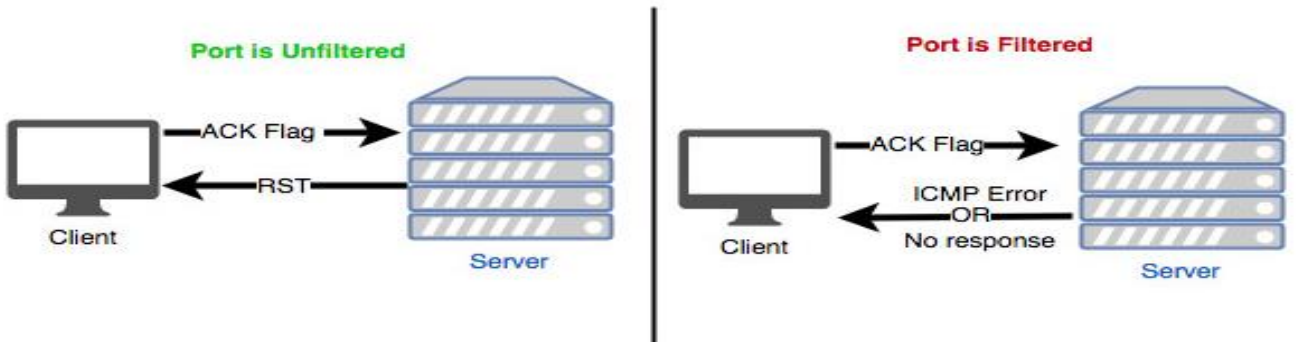
## ACK SCAN

Bir TCP ACK taraması gerçekleştirirken, Nmap bir hedefi sorgular ve RST yanıtlarını arar. Herhangi bir yanıt alınmazsa, sistem filtrelenmiş olarak kabul edilir. Sistem bir RST paketi döndürürse, filtrelenmemiş olarak etiketlenir. Filtrelenmemiş portların anlamı hedefin güvenlik duvarında açık veya kapalı olmasını sağlayan özel kuralların olması muhtemeldir.

**NOT: -sA seçeneği, filtrelenmemiş bağlantı noktalarının açık veya kapalı olmasına bakmaz. Tek amacı sistemde filtreleme cihazı olup olmadığını belirlemektir.**

**sA seçeneği bir TCP ACK taraması yapar. Kullanım Şekli : nmap -sA [hedef]**

**-sA seçeneği, hedef sistemin bir güvenlik duvarı tarafından korunup korunmadığını belirlemek için kullanılabilir.**



## Temel Tarama Teknikleri

**Tek bir hedefi taramak için:**

**nmap hedef\_ip\_adresi**

**Birden fazla hedefi taramak için:**

**nmap hedef1\_ip hedef2\_ip hedef3\_ip**

**IP adresi aralığını taramak için:**

**nmap 192.168.1.1-50**

**Bir alt ağı taramak için:**

**nmap 192.168.1.0/24**

**Birden fazla alt ağı taramak için:**

**nmap 192.168.1.0/24 10.0.0.0/24**

**Hedefleri bir dosyadan okumak için:**

**nmap -iL hedef dosya.txt**

'hedef dosya.txt' adlı bir dosyaya hedef IP'leri veya alan adlarını ekleyin.

**Taramadan belirli bir hedefi hariç tutmak için:**

**nmap 192.168.1.0/24 --exclude 192.168.1.5**

**Rastgele birkaç hedefi taramak için:**

**nmap -iR 5**

Burada "5" rastgele tarama için belirlenen hedef sayısıdır.

## PORT SPECIFICATION

**Tek bir portu taramak için (örneğin, 80. port):**

**nmap -p 80 hedef\_ip\_adresi**

**Birden fazla belirli portu taramak için (örneğin, 80, 443 ve 8080):**

**nmap -p 80,443,8080 hedef\_ip\_adresi**

**Belirli bir port aralığını taramak için (örneğin, 20 ile 1000 arası):**

**nmap -p 20-1000 hedef\_ip\_adresi**

**Belirli bir portu hariç tutmak için (örneğin, 80. portu hariç tut):**

**nmap --exclude-ports 80 hedef\_ip\_adresi**

**Bilinen yaygın portları taramak için (Top 1000 port):**

**nmap -p 1-1000 hedef\_ip\_adresi**

**Tüm portları taramak için (0 ile 65535 arası):**

**nmap -p- hedef\_ip\_adresi**

ÖZELLİK	SEÇENEK
Hızlı Tarama Yapma	-F
Belirli Portları Tarayın	-p [port]
Portlarıİsme Göre Tarama	-p[name]
Protokollere Göre Portları Tarama	-p U:[UDP ports],T:[TCP ports]
Tüm Portları Tara	-p “*”
Sık Kullanılan Portları Tara	--top-ports [number]
Ardışık Bağlantı Noktalı (Port)Tarama Yapma	-r

## HOST DISCOVERY

**Nmap'te ana bilgisayar keşfi, daha fazla tarama yapmadan önce bir ağdaki canlı ana bilgisayarların tanımlanması sürecini ifade eder.**

**Standart host keşfi (ICMP ping):**

**nmap -sn hedef\_ip\_adresi**

**TCP SYN ping ile host keşfi:**

**nmap -PS hedef\_ip\_adresi**

**TCP ACK ping ile host keşfi:**

**nmap -PA hedef\_ip\_adresi**

**UDP ping ile host keşfi:**

**nmap -PU hedef\_ip\_adresi**

**ICMP echo request ile host keşfi:**

**nmap -PE hedef\_ip\_adresi**

**ARP ping ile host keşfi:**

**nmap -PR hedef\_ip\_adresi**

**ICMP, TCP SYN, TCP ACK, UDP, ARP ping tümüyle birleştirilmiş host keşfi:**

**nmap -PE -PS -PA -PU -PR hedef\_ip\_adresi**

**Tarama sırasında DNS sorgularını kullanarak hedefleri çözmek:**

**nmap -sL hedef\_ip\_adresi**

## **İŞLETİM SİSTEMİ VE SERVİS KEŞFİ**

### **İşletim Sistemi Algılama**

**-O parametresi, Nmap'ın işletim sistemi algılama özelliğini etkinleştirir.**

**Kullanım Şekli : nmap -O [hedef]**

**OS algılamasının düzgün çalışabilmesi için, hedef sistemde en az bir açık ve bir kapalı port olmalıdır.**

**Nmap OS'ü doğru şekilde tanımlayamazsa, --osscan-guess seçeneğini kullanarak onu tahmin etmeye zorlayabilirsiniz.**

**Kullanım Şekli : nmap -O --osscan-guess [hedef]**

### **Servis Sürüm Algılama**

**-sV parametresi Nmap'ın servis versiyonu algılama özelliğini etkinleştirir.**

**Kullanım Şekli : nmap -sV [hedef]**

ÖZELLİK	SEÇENEK
İşletim Sistemi Algılama	-O
Bilinmeyen bir OS tahmin etmeye çalışmak	--osscan-guess
Servis Sürüm Algılama	-sV
RPC Taraması gerçekleştirme	--version-trace
Sürüm Taramalarında Sorun Giderme	-sR

### **ZAMANLAMA SEÇENEKLERİ**

<b>Minimum Host Grubu Boyutu</b>	--	<b>min-hostgroup</b>
<b>Maksimum Host Grubu Boyutu</b>	--	<b>max-hostgroup</b>
<b>Minimum Paket Hızı</b>	--	<b>min-rate</b>
<b>Maksimum Paket Hızı</b>	--	<b>max-rate</b>



Şablon	İsim	Açıklama
-To	Paranoyak	Son derece yavaş
-T1	Sinsi	İzinsiz giriş tespit sistemlerinden kaçınmak için kullanışlıdır
-T2	Kibar	Hedef sisteme müdahale olasılığı düşük
-T3	Normal	Varsayılan zamanlama şablonu
-T4	Agresif	Yerel ağlarda daha hızlı sonuçlar üretir
-T5	Çılgın	Çok hızlı ve agresif tarama

## **FIREWALL ATLATMA**

**Firewall'lar, ağ trafiğini kontrol eden ve güvenlik politikalarını uygulayan güvenlik cihazlarıdır. Nmap taraması yapan bir sistem, hedef ağdaki cihazlara ulaşmak için çeşitli ağ paketleri gönderir. Ancak, firewall'lar genellikle gelen ağ trafiğini denetler ve buna göre izin verilen veya engellenen trafiği belirler. Ancak Nmap kendi bünyesinde bulunan bazı seçenekler vasıtasıyla bu güvenlik ürünlerini atlatabilir. Fragmantasyon, spoofing ve packet**

**manipulating seçenekleri vasıtasıyla Nmap güvenlik ürünlerini atlatıp, taramalarını daha rahat bir şekilde gerçekleştirebilir.**

#### **Fragmentation (Fragmantasyon):**

**Nmap, tarama paketlerini daha küçük parçalara bölmek ve ağdaki güvenlik aygıtlarını atlatmak için fragmentasyon özelliğine sahiptir. Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, 8 byte olması isteniyorsa aşağıdaki komut kullanılmalıdır**

```
nmap -f [hedef]
```

**Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, el ile girilerek belirlenmek isteniyorsa aşağıdaki komut kullanılmalıdır:**

```
nmap - - mtu <sayi> [Hedef_IP]
```

#### **Spoofing (Sahte Kimlik Kullanma):**

**Nmap, kullanıcının IP adresini gizleyerek ve başka bir kaynaktan geliyormuş gibi davranarak, hedef sistem üzerinde iz bırakmadan tarama yapma yeteneğine sahiptir.**

```
nmap -S [sahte_kaynak_IP] [hedef]
```

#### **Packet Manipulation (Paket Manipülasyonu):**

**Nmap, kullanıcıların tarama paketlerini özelleştirmelerine izin verir. Bu, belirli protokol başlıklarını değiştirme ve özelleştirme amacı taşır.**

```
nmap --data-length [uzunluk] [hedef]
```

### **NMAP TARAMA ÇIKTISINI DOSYAYA YAZDIRMAK**

#### **Normal Metin Çıktısı (TXT dosyası):**

```
nmap -oN /path/to/output.txt [hedef]
```

#### **XML Çıktısı:**

**nmap -oX /path/to/output.xml [hedef]**

**Grepable Çıktı:**

**nmap -oG /path/to/output.grep [hedef]**