

NMAP - Network Mapper




Ondokuz Mayıs Üniversitesi
Siber Güvenlik Topluluğu


NMAP Nedir ?

Nmap, bilgisayar ağıları uzmanı Gordon Lyon (Fyodor) tarafından geliştirilmiş bir güvenlik tarayıcısıdır. Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir.





Nmap kullanarak ağıba bağlı herhangi bir bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılımların sürüm numaraları, bilgisayarın güvenlik duvarına sahip olup olmadığı, ağ kartının üreticisinin adı gibi bilgiler öğrenilebilmektedir.



NMAP Kullanım Alanları

- Taranan ağ üzerindeki sistemler hakkında bilgi sahibi olunmasında(port, üzerinde koştan uygulama vb. bilgileri öğrenmek gibi).
- Ağ topolojisinin çıkarılmasında.
- Sızma testlerinin gerçekleştirilmesinde.
- Herhangi bir ağ hazırlanırken gerekli ayarların test edilmesinde.
- Ağ envanteri tutulması, haritalaması, bakımında ve yönetiminde.

NMAP KULLANIMI

Nmap kullanırken aşağıdaki gibi bir dizim uygun olacaktır.

nmap [tarama türü] [opsiyonlar] [hedef tanımlama]



HEDEF TANIMLAMA

Nmap kullanırken hedefi birçok şekilde tanımlayabilirsiniz. Örneklerle inceleyebiliriz:

nmap 192.168.133.1 #Tek bir IP adresi için tarama yapılacağını belirtir

nmap 192.168.133.1-10 # 192.168.133.1 ve 192.168.133.10 adres aralığında ki tüm IP adreslerini tarar.

nmap escoder.net # Domain taraması yapar

nmap -iL ipadresleri.txt # ipadresleri.txt dosyası içerisinde ki IP adreslerini tarar

nmap -p 443 -iR 10 #HTTPS servisini kullanarak 10 adet host tarar

nmap *.*.1.5 #1.0.1.5 – 255.255.1.5 aralığındaki her şeyi tarar

nmap 192.168.1-2.* #192.168.1.0 – 192.168.2.255 aralığındaki her şeyi tarar.

nmap -- exclude escoder.net,Cyber-warrior.org 192.168.1.0/24 #escoder.net ve Cyber-warrior.org siteleri haricinde ki tüm ip adreslerini tarar (Reverse IP Lookup).

KEŞİF AŞAMASI(HOST DISCOVERY)

Ağda bulunan ve çalışan cihazların testi için farklı tarama yöntemleri bulunmaktadır. Aşağıdaki örnekleri inceleyebilirsiniz.

Ping Sweep | `nmap -sP 192.168.133.0/24`

| Tüm Sistemlere Ping atarak yanıt veren sistemlerin açık olup olmadığını denetler, bir nevi sunucu ve istemcileri tespit eder.

Ping SYN | `nmap -PS 192.168.133.0/24`

| TCP SYN Ping paketleri ile sistemlerin açık olup olmadığını denetler

Ping ACK | `nmap -PA 192.168.133.0/24`

| TCP ACK Ping paketleri ile sistemlerin açık olup olmadığını denetler



KEŞİF AŞAMASI(HOST DISCOVERY)

Ping UDP | nmap -PU 192.168.133.0/24

| UDP Ping paketleri ile sistemlerin açık olup olmadığını denetler

Ping ICMP | nmap -PE 192.168.133.0/24

| ICMP Echo Request paketlerini kullanarak sistemlerin açık olup olmadığını denetler

Ping ARP | nmap -PR 192.168.133.0/24

| ARP Ping paketlerini kullanarak sistemlerin açık olup olmadığını denetler



KEŞİF AŞAMASI(HOST DISCOVERY)

Traceroute | nmap -traceroute 192.168.133.0/24

| Traceroute özelliğini aktifleştirerek hedefe giden paketlerin yol analizini yapar

DNS Keşfi | nmap -system-dns 192.168.133.0/24

| İşletim sistemi üzerinde ki DNS Serverları kullanır

Reverse DNS Keşfi | nmap -R 192.168.133.0/24

| IP adresinden hostname bilgisi elde edilmesin için kullanılır.



PORT TARAMA TEKNİKLERİ

NMAP üzerinde, portların durumunu ifade eden 6 tanımlama mevcut.

Open | Port açıktır ve açık portu dinleyen bir uygulama vardır.

Closed | Port kapalıdır ancak erişilebilir. Dinleyen herhangi bir uygulama yoktur.

Filtered | Filtrelerden ötürü NMAP portun durumunu çözmemiştir.

Unfiltered | ACK Scan sonuçlarında karşımıza çıkan bu tanımlamada, portun erişilebilir olduğunu ancak açık olup olmadığı tespit edilememiştir.

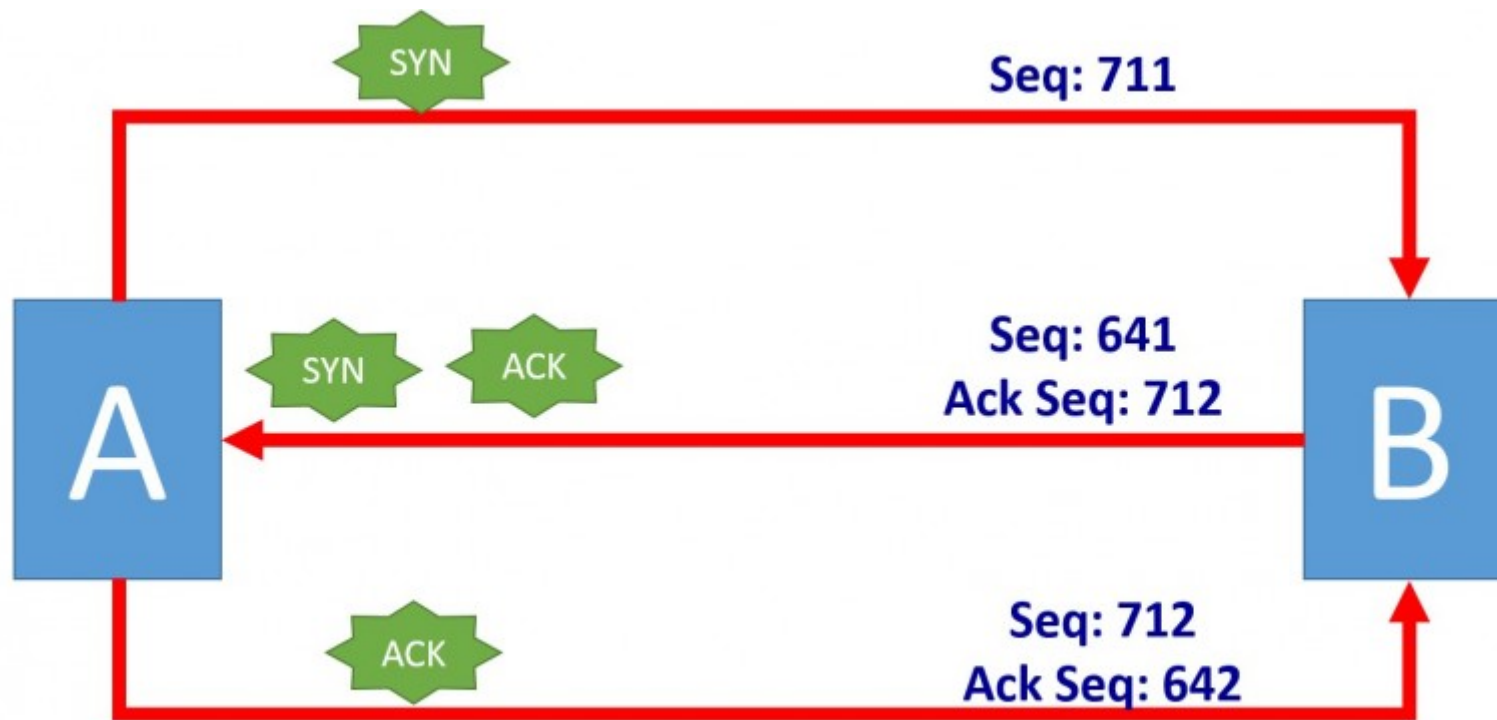
Open Filtered | UDP, IP Protocol, FIN, NULL ve XMAS Scan için dönen bu durumda portların açık veya filtrelenmiş olduğu tespit edilememiştir.

Closed Filtered | IDLE Scan için dönen bu durumda portların kapalı yada filtrelenmiş olduğu tespit edilememiştir.



PORT TARAMA TEKNİKLERİ

3-Way Handshake(3 yollu el sıkışma)



PORT TARAMA TEKNİKLERİ

TCP SYN Scan

NMAP üzerinde varsayılan tarama tekniği SYN Scandır. Oldukça hızlı olan bu tarama tekniği için 3 adet dönüş olacaktır; open, closed, filtered.

Bir diğer adı ise Half Open Scan'dır (Yarı Açık Tarama). Bu ismi almasının nedeni, 3 yollu el sıkışmasının tamamlanmamasıdır. Böylece hedef sistemde oturum açılmaz dolayısı ile kayıt tutulmaz.

Kaynak makinenin TCP Syn bayrağı göndermesiyle karşı tarafın TCP portlarının açık veya kapalı olduğu dönen bayrağın RST+ACK veya SYN+ACK olmasından anlaşılır. RST+ACK dönüyorsa kapalı, SYN+ACK dönüyorsa açık anlamına gelir.

Kullanımı: **nmap -sS -v [hedef ip]**

PORT TARAMA TEKNİKLERİ

TCP Connect Scan

Başlıktaki "connect" kısmından da anlaşılacağı gibi, SYN Scan tekniğinin tam tersi bir şekilde 3 yollu el sıkışma işlemi gerçekleşir ve tarama kayıt altına alınır. SYN Scan tekniğinin tersine eğer SYN paketlerine karşılık SYN+ACK geliyorsa ACK paketi gönderir ve port tarama tamamlanır.

Kullanım: **nmap -sT [hedef ip]**



PORT TARAMA TEKNİKLERİ

UDP Scan

UDP portlarının durumunu analiz etmek için kullanılan bu yöntemde tarama gönderilen UDP paketlerinin durumuna göre gerçekleşir. ICMP Port Unreachable ise port kapalıdır, eğer gelen cevap yine UDP paketi ise port açıktır.

Kullanım: **nmap -sU [hedef ip]**



PORT TARAMA TEKNİKLERİ

NULL - FIN - XMAS Scan

3 tarama türü de kısmi benzerlik göstermektedir. Gönderilen paketlere cevap olarak RST+ACK gönderiliyorsa port kapalı, ICMP Port Unreachable gönderiliyorsa port filtreli, hiç bir şey gönderilmiyorsa port açıktır.

NULL Scan üzerinden gönderilen paketler her hangi bir bayrağa sahip değildir (her hangi bir teknik uygulanmaz).

FIN Scan üzerinden gönderilen paketler FIN bayrağına sahiptirler (kendi tekniğini uygular).

XMAS Scan üzerinden gönderilen paketler, farklı bayraklara sahip olabilir.

Kullanım: **nmap -sN [hedef ip] #Null Scan**

Kullanım: **nmap -sF [hedef ip] # FIN Scan**

Kullanım: **nmap -sX [hedef ip] # XMAS Scan**

PORT TARAMA TEKNİKLERİ

ACK - Window Scan

ACK Scan, güvenlik duvarının yapılandırmasını incelemek için sıkça kullanılan yöntemlerden biridir. ACK bayraklı gönderilen paketlere gelen duruma göre portun durumu analiz edilir.

Gönderilen paketlere RST geri dönüyorsa portun Unfiltered olduğu ortaya çıkar. Eğer ICMP Unreachable paketi dönüyorsa yada bir şey dönmüyorsa portun filtered olduğu ortaya çıkar.

Window Scan ise, ACK taramasından farklı olarak portların açık olup olmadığını anlayabilir.

Kullanım: **nmap -sA [hedef ip]# ACK Scan**

Kullanım: **nmap -sW [hedef ip] # Window Scan**

Ping Scan

Tek bir ICMP Echo paketi gönderilen bu taramada ICMP filtre bulunmadığı sürece bize ICMP Echo cevabı dönecektir.

Kullanım: **nmap -sP[hedef ip]**

IP Protocol Ping Scan

IP üzerinden gerçekleştirilen bu taramada, erişilemeyen IP adresi cevap vermeyecektir. Erişilebilen IP ise RST tipi bayrak döndürecektir.

Kullanım: **nmap -sO [hedef ip]**

PORT TANIMLAMA

Hedef tanımlama kısmında yaptığımız tanımlama da "dikkat edilmesi gereken nmap bize en bilindik portları taradı" demiştik. Evet, eğer herhangi bir parametre verilmezse NMAP bize en bilindik portları hızlı bir biçimde tarar. Sizler ise vereceğiniz parametreler ile bu tarama işlemini özelleştirebilirsiniz.

nmap -sS -F 192.168.133.129 # En yaygın 100 portu tara

nmap -sS -p80 192.168.133.129 # 80 portunu tara

nmap -sS -p1-100 192.168.133.129 # 1 ile 100 arasında ki portları tara

nmap -sS -p1,100,102 192.168.133.129 # 1, 100 ve 02. portları tara

nmap -sS -top-ports <n> 192.168.133.129 # En sık kullanılan n adet portu tarar

nmap -sS -p- 192.168.133.129 # 65535 adet portun tamamını tarar

nmap -sS -p U:53,T:22 192.168.133.129 # UDP 53 ve TCP 22. portu tarar

SERVİS VE VERSİYON KEŞFİ

Yapılan port taramadan elde edilen bilgiler birçok zaman bize yetmeyecektir. Orada hangi servisin çalıştığı ve servisin hangi versiyonunun kullanıldığını bilmek, hedefi tanıma aşamasında bizi bilgili kılacaktır. Bunun için aşağıdaki parametre işimize yarayabilir.

Tarama Türü İçin Parametre: -sS # SYN Scan

Versiyon Tespiti İçin Parametre: -sV

Kullanım: **nmap -sS -sV 192.168.133.129**



İŞLETİM SİSTEMİ ANALİZİ

NMAP yetenekli bir yazılımdır, bize kullanılan işletim sistemi hakkında da detaylı bir rapor sunabilir, bu analizler bizim için değerli sonuçlar olabilir. İşletim sisteminin tespiti için nmap tarama esnasında minimum bir açık bir kapalı port bulunmalıdır. 2 adet komut kullanılabilir bu durumlarda.

İşletim Sistemi Analizi İçin Parametre: -O

Kullanım: **nmap -sS -O 192.168.133.129**

Kullanım: **nmap -sS -A 192.168.133.129**

ÇIKTILARI AYARLAMA

NMAP yazılımının sahip olduğu yeteneklerden biri de çıktıları istediğimiz yönde alabilmemizdir. Örneğin çıktıyı kaydetmek için TXT, Metasploitte kullanabilmek için XML şeklinde alabiliriz.

nmap -sS -oN cikti.txt 192.168.133.129 # TXT biçiminde, normal NMAP çıktısı verir

nmap -sS -oX cikti.xml 192.168.2.1 # XML biçiminde bir çıktı üretir, Metasploit için ideal bir komut.

nmap -sS -oG cikti.txt 192.168.2.1 # Düzenlenebilir NMAP çıktısı verir (ne işe yaradığı konusunda en ufak bir fikrim yok)

nmap -sS -oA dosyaismi 192.168.2.1 # Tüm biçimlerde çıktı verir.

İpucu: -oA parametresi ile yapılan işlemde tarama durursa "nmap -resume dosyaismi" denilerek taramaya devam edilebilir.

SPOOFİNG

NMAP güvenlik nedeni ile tarama işlemini farklı bir bilgisayardan yapıyormuş gibi gösterebilir. Önemli olan nokta belirtilecek sistemin IP adresi ile hedef sistemin uyumlu olmasıdır. Özel IP kullanan LAN ortamının Reel IP kullanması pek mantıklı olmayacaktır. Eğer IP adresi belirtilemez ise NMAP rast gele olarak IP adresi seçecektir.

Kullanım: **nmap -D <gösterilecek_ip> <hedef_ip>**

Kullanım: **nmap -D 192.168.133.1 192.168.133.129**

NMAP yazılımının ethernet kart arayüzünün IP adresini bulamadığı durumlarda -e (interface) parametresini kullanarak IP adresi atanabilir.

Kullanım: **nmap -D <gösterilecek_ip> -e <interface> <hedef_ip>**



PAKET MANİÜLASYONU

Güvenlik ürünlerini atlatmak için, Nmap çok fazla sayıda packet manipulating özelliği barındırır. Aşağıda bu özellikler ve açıklamaları bulunmaktadır :

--data-length <sayı> # Paket boyutunun olacağı uzunluğu <sayı> belirtir.

--ip-options <R|T|U|S *IP IP2...+ |L *IP IP2 ...+ > yada --ip-options <hex string> # Paketler içerisindeki IP özelliklerini belirtir.

--randomize-hosts # Listede belirtilen taranılacak hostları rastgele bir şekilde seçer.

--badsum # Yanlış checksuma sahip TCP veya UDP paketleri gönderir.

KOMBİNASYONLAR

nmap-update # NMAP yazılımını güncellemek için kullanılır.

nmap -h # Yardım metinleri, kategorik bir biçimde tüm özellikler ekrana dökülecektir.

nmap -sS -v 192.168.133.129 # bu komutta yabancı gelen tek şey -v parametresi. Özelliği NMAP yazılımının ekrana daha fazla bilgi dökmesini sağlar.

nmap -sS -sV -Pn -p- 192.168.133.129 # Standart SYN Scan ile tarama yapacak ve versiyon tespitinde bulunacaktır. Bilmediğimiz ise -Pn komutu ping atmasını önlemek ve -p- komutu ise 65535 portun tamamını taramasını sağlayacaktır.

nmap -sW -T1 -p- 192.168.133.129 # Window Scan gerçekleştirecek yazılım, -T1 komutu ile yavaş bir şekilde tarama yapacak ve Firewall yani güvenlik duvarlarına yakalanamayacaktır.

nmap -script vuln 192.168.10.0/24 # Bu komut ile NMAP içeriğinde ki exploiteri hedef sistem üzerinde test edecek ve sonuçları ekrana dökülecektir.

nmap -script=ftp-brute -p 21 192.168.133.129 # NMAP, içinde ki ftp-brute yazılımı ile hedef makinanın 21. portuna elinde ki şifreler ile giriş yapmaya çalışacaktır. Bu Brute/Force yani Kaba/Kuvvet saldırılarına girer. Bu yazılımları seçmek için -script=yazılım-ismi denilmesi yeterlidir.

nmap -sC 192.168.44.3 # NMAP içerisinde ftp-brute gibi onlarca script bulunmaktadır. Bu komut ile NMAP, içeriğinde ki tüm scriptleri çalıştıracaktır.



Sunumu hazırlarken faydalandığım kaynaklar;

<https://nmap.org/>

<https://blogs.sans.org/pentesting/files/2013/10/NmapCheatSheetv1.0.pdf>

<https://www.cyberciti.biz/networking/nmap-command-examples-tutorials/>

<https://pentestlab.blog/>

