1)

Başlıca görevi port taraması olan Nmap yazılımının diğer özellikleri şunlardır:

- Versiyon Tespiti
- İşletim Sistemi Tespiti
- Çalışan Aygıt Tespiti, çalışma Süreleri
- Yazılımların Kullandıkları Servis (Port) Tespiti
- Yazılımların Versiyon Numaraları Tespiti
- Yazılım Zafiyet Tespitleri
- Bilgisayarın Güvenlik Duvarı (Firewall) Tespiti
- Ağ Kartı Üreticisinin Adı

2)

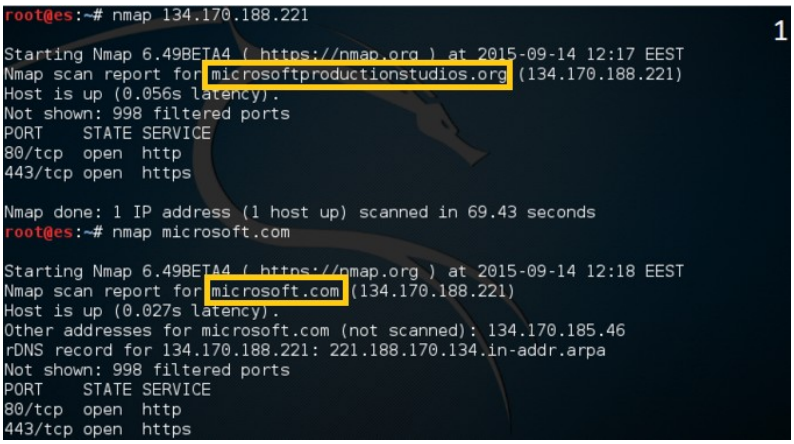
Nmap yaklaşık 15 farklı tarama yöntemi ve her tarama için yaklaşık 20 farklı seçeneğe sahiptir.

3)

Taranacak hedef sistemin ismi girilirse NMAP öncelikle DNS Lookup işlemi yapacaktır. Bu bir NMAP fonksiyonu değildir. DNS sorgularının network trafiğinde görülmesinden dolayı tüm işlemler kayıt altına alınır (loglanır). Eğer isim yerine IP adresi girilirse kayıt tutma işlemi yapılmayacaktır.

4)

Domain ve IP sorgularında gelen sonuçlar birbirlerinden farklı olabilir. Örneğin;



Görüldüğü gibi ilk çıktıda Microsoft.com'un ip'si kullanılmış olmasına rağmen Nmap scan report for microsoftprodictionstudios.org diyerek farklı bir alan adı taraması yapılmıştır. Ancak IP adresi yerine direk alan adı (domain) taraması yapıldığında ise bize bir önceki taramada kullandığımız IP adresini göstermiştir.

5)

Nmap Syntax

Nmap <tarama türü> <seçenekler> <hedef>

Tarama türünü gönderilecek paketin içerdiği flag/bayrak belirler.

Seçenekler ise yapılacak işlemi belirtir. Mesela port analizi, işletim sistemi keşfi, versiyon tespiti, vs…

6)

Taramalar sonucu portların durumunu ifade eden 6 tanımlama mevcuttur:

a. Open

Port açıktır ve uzak sistemde bu açık portu dinleyen bir uygulama vardır.

b. Closed

Port kapalıdır, ancak erişilebilirdir. Bu portu dinleyen herhangi bir uygulama yoktur.

c. Filtered

Filtrelerden - mesela firewall'lardan - ötürü Nmap portun durumunu çözememiştir.

d. Unfiltered

ACK Scan taramalarında karşımıza çıkan bu tanımlama portun erişilebilir olduğunu, ancak açık olup olmadığının tespit edilemediğini, ayrıca filtered olup olmadığının da tespit edilemediğini belirtilir.

e. Open | Filtered

UDP, IP Protocol, FIN, NULL ve XMAS gibi taramalarda portun açık veya filtrelenmiş olup olmadığının tespit edilemediğini belirtir.

f. Closed | Filtered

IDLE taraması sonucu dönebilen Closed Filtered durumu portların kapalı ya da filtreli olup olmadığının tespit edilemediğini belirtir.

7)

Ağda bulunan ve çalışan cihazların keşfi için Nmap'in kullandığı tarama türleri:

a. Ping Sweep | nmap -sP 192.168.133.0/24

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

b. Ping SYN | nmap -PS 192.168.133.0/24

TCP SYN Ping paketleri ile sistemlerin açık olup olmadığı denetler.

c. Ping ACK | nmap -PA 192.168.133.0/24

TCP ACK Ping paketleri ile sistemlerin açık olup olmadığını denetler.

d. Ping UDP | nmap -PU 192.168.133.0/24

UDP Ping paketleri ile sistemlerin açık olup olmadığını denetler.

e.Ping ARP | nmap -PR 192.168.133.0/24

ARP Ping paketlerini kullanarak sistemlerin açık olup olmadığını denetler.

f. Traceroute | nmap --traceroute 192.168.133.0/24

Traceroute özelliğini aktifleştirerek hedefe giden paketlerin yol analizini yapar.

g. DNS Keşfi | nmap --system-dns 192.168.133.0/24

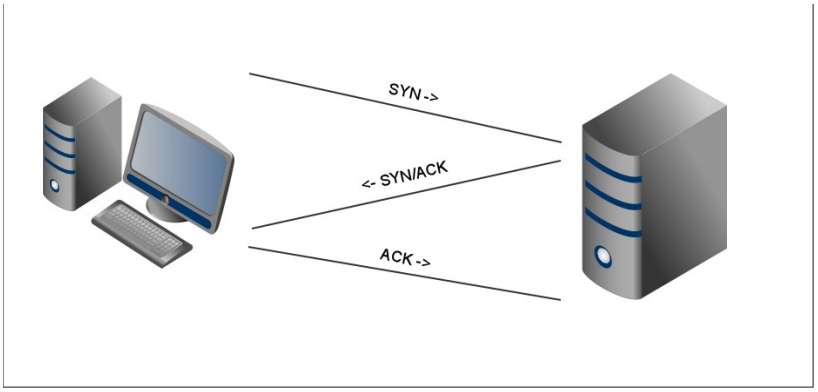
İşletim sistemi üzerindeki DNS server'ları keşfeder.

h. DNS Çözümleme | nmap -R 192.168.133.0/24

Her daim IP adresinden domain adı çözümlemesi yaparak tarama yapar. -n kullanılsaydı asla çözümleme yapma denmiş olurdu. İkisi de kullanılmazsa varsayılan durum yeri geldiğinde çözümleme yaptır.

ı. TCP SYN Scan | nmap -sS 192.168.133.129

NMAP üzerinde varsayılan tarama tekniği SYN Scandır. Oldukça hızlı olan bu tarama tekniği için 3 adet dönüş olacaktır; open, closed, filtered. Bu taramanın bir diğer adı ise Half Open Scan'dır (Yarı Açık Tarama). Bu ismi almasının nenedi TCP 3 yollu el sıkışmasının tamamlanmamasıdır. Böylece hedef sistemde oturum açılmaz dolayısı ile kayıt tutulmaz.



TCP SYN Scan'da gönderilen SYN paketine karşılık gelen cevap RST+ACK ise port kapalıdır. Eğer alınan yanıt SYN+ACK ise portun açık olduğu anlaşılır ve bir RST paketi gönderilerek iletişim kurulmadan tarama işlemi tamamlanır.

i. TCP Connect Scan | nmap -sT 192.168.133.129

TCP SYN Scan tekniğinin tersine eğer SYN paketlerine karşılık SYN+ACK geliyorsa ACK paketi gönderilir ve tarama tamamlanılır. Yani bu tekniğin ismindeki Connect kelimesinden de anlaşılabileceği gibi TCP 3 Yollu El Sıkışma işlemi gerçekleştirilir ve tarama kayıt altına alınır.

j. UDP Scan | nmap -sU 192.168.133.129

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.

k. NULL, FIN ve XMAS Scan

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

NULL Scan | nmap -sN 192.168.133.129

Bu tarama üzerinden gönderilen paketler herhangi bir bayrağa sahip değildir (herhangi bir teknik uygulanmaz).

FIN Scan | nmap -sF 192.168.133.129

Bu tarama üzerinden gönderilen paketler FIN Bayrağına sahiptirler (kendi tekniğini uygular).

XMAS Scan | nmap -sX 192.168.133.129

Bu tarama üzerinden gönderilen paketler farklı bayraklara sahip olabilir.

l. ACK Scan | nmap -sA 192.168.133.129

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 ya da bir şey dönmüyorsa portun filtered olduğu ortaya çıkar.

m. Window Scan | nmap -sW 192.168.133.129

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

n. Ping Scan | nmap -sP 192.168.133.129

Tek bir ICMP Echo paketi gönderilir. Uzak sistemde ICMP Filtresi bulunmadığı sürece bize ICMP Echo cevabı dönecektir. Böylece ICMP Filtre var mı yok muyu anlayabiliriz.

o. IP Protocol Ping Scan

IP üzerinden gerçekleştirilen bu taramada, erişilemeyen IP adresi cevap vermeyecektir. Erişilebilen IP ise RST bayraklı paket gönderecektir. Böylece IP'nin erişilebilir olup olmadığı tespit edilir.

8)

Eğer herhangi bir parameter girilmezse Nmap bize en bilindik portları tarayacaktır.

nmap 192.168.133.129

Çok sayıda filtered port olduğunda nmap sonuçları göstermeyip sadece 999 Filtered Port gibi

bildirimler vermektedir. Tümünün açık seçik gösterilmesi istenirse -dd parametresi kullanılır.

nmap -dd www.karabuk.edu.tr

En yaygın 100 portu tarar

nmap -F 192.168.133.129

Spesifik servis taraması yapar.

nmap -p http,mysql,ftp www.ubys.net

Sadece açık portları görüntüler (filtered ve closed görünmez).
nmap --open www.ubys.net

Çoklu domain taraması yapar. Mesela
nmap www.includekarabuk.com www.karabuk.edu.tr www.ubys.net

Aralık tayin ederek tarama yapar. Mesela
nmap 192.168.2.1-6 // 192.168.2.1'den 192.168.2.6'ya kadar tarama yapılır

Tüm subnet'i taramak istersek aralık 0-255 yapılmalıdır ya da * kullanılmalıdır ya da /24
kullanılmalıdır. Böylece her host için ayrı ayrı port/servis taraması yapılır.
nmap 192.168.2.0-255
nmap 192.168.2.*
nmap 192.168.2.1/24

Dosyada satır satır sıralanmış IP adreslerini tarar.
nmap -iL targets.txt // import from list

80nci portu tarar
nmap -p 80 192.168.133.129

1 ile 100 arasındaki portları tarar
nmap -p 1-100 192.168.133.129

1nci, 100ncü, 101 ile 105 arasındakileri ve 109ncu portları tarar
nmap -p 1,100,101-105,109 192.168.133.129

En sık kullanılan mesela 10 adet portu tarar
nmap --top-ports 10 192.168.2.1 // SYNTAX: nmap --top-ports <n> 192.168.133.129

65535 adet portun tamamını tarar

nmap -p- 192.168.133.129

UDP 53 ve TCP 22. portu tarar

nmap -p U:53,T:22 192.168.133.129

9)

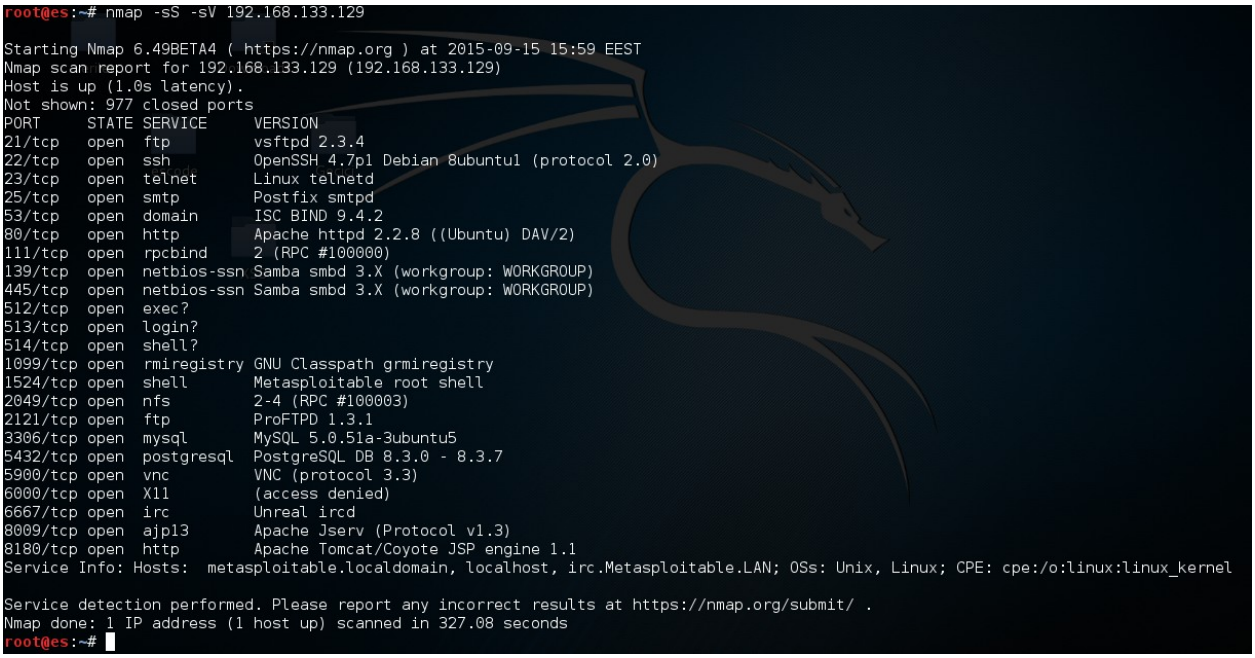
Servis ve Versiyonlarının Keşfi

Taranan portları dinleyen (kullanan) yazılımları ve bunların versiyonlarını öğrenirsek metasploit'te bu kriterlere göre exploit arattırabiliriz ve eğer exploit bulursak uzak sistemi hack'leyebiliriz. Servis ve versiyon keşfi için kullanılan parametreler:

Tarama Türü için Parametre : -sS // SYN Scan

Versiyon tespiti İçin Parametre : -sV

Nmap -sS -sV 192.168.133.129



10)

İşletim Sistemi Analizi

İşletim sistemi analizi için -O parametresi kullanılır. Daha sıkı bir tarama için -A parametresi kullanılır.

nmap -sS -O 192.168.133.129

nmap -sS -A 192.168.133.129

Bu taramalar bize oransal sonuçlar verecektir.

11)

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

Tarama çıktısını cikti.txt adlı dosyaya yazdırır.

nmap -oN cikti.txt 192.168.133.129

XML biçiminde bir çıktı üretir, Metasploit için ideal bir komuttur.

nmap -oX cikti.xml 192.168.2.1

13)

Kullanışlı Örnekler

Window Scan taraması --T1 komutu ile yavaş bir şekilde gerçekleşir ve böylece Firewall, yani

güvenlik duvarlarına yakalanılmaz.

nmap --sW --T1 -p- 192.168.133.129

Bu komut ile NMAP içeriğindeki exploitler hedef sistem üzerinde test edilecektir ve sonuçları
ekrana dökecektir.

nmap --script vuln 192.168.10.0/24

NMAP içindeki ftp-brute yazılımıyla hedef makinanın 21. portuna wordlist kullanarak brute
force yapar. Nmap içerisindeki alt yazılımları seçmek için --script=yazilim-ismi denilmesi
yeterlidir.
nmap --script=ftp-brute -p 21 192.168.133.129

NMAP içerisinde ftp-brute gibi onlarca script bulunmaktadır. Bu komut ile NMAP yazılımı
içeriğindeki tüm scriptleri hedef üzerinde deneyecektir.

nmap -sC 192.168.44.3

-sS (TCP SYN Scan) yaparken -v kullanırsak Nmap tarama esnasında neleri yapıyor sorusunun
cevabını ekrana yansıyan bilgilendirici bildirimlerle öğrenebiliriz.

nmap -sS -v 192.168.133.129

Standart SYN Scan ile tarama yapacak ve versiyon tespitinde bulunacaktır. Bilmediğimiz ise -
Pn komutu ping atmasını önleyecektir ve -p- komutu ise 65535 portun tamamının taranmasını
sağlayacaktır.

nmap -sS -sV -Pn -p- 192.168.133.129

Kaynak: http://www.illeg4lizm.com/konu-nmap-kullanimi-genis-anlatim.html

Kaynak: https://www.youtube.com/playlist?list=PL6gx4Cwl9DGBsINfLVidNVaZ-7_v1NJIo