Nmap Cheat Sheet [TR]

Bu yazımda sizlere pentest aşamalarında veya CTF yarışmalarında “nmap” aracını kullanırken kolaylık sağlaması açısında bir cheet sheet yani kopya kağıdı hazırlamaya çalıştım. Bunun için de elimden geldiğince örnekler vermeye ve farklı noktaları göstermeye çalıştım.

Nmap aracı ağ taramaları için kullanılan bir zafiyet keşif aracıdır. Taradığınız sistem veya ağ hakkında sizlere faydalı olacak bilgiler sunar. Elde ettiğiniz bu bilgiler ile kendinize bir saldırı rotası çizebilirsiniz.

Nmap taraması ile elde edebileceğiniz bazı bilgiler şunlardır:

1) **Sistemde açık bulunan port numaraları**

2) **Açık bulunan portlarda çalışan servisler**

3) **Çalışan servislerin versiyon numaraları**

4) **İşletim sistemi hakkında bilgiler**

Tabiki de bu bilgileri elde etmek için “nmap” sorgusunu konfigüre etmeyi bilmeniz gerekmektedir. Bu yazımda da sizlere bu konfigürasyonları nasıl yapacağınıza yol göstermeye çalışacağım. Ben buradaki bilgileri nmap için yazılmış “help” menüsünden ulaştım. Siz de bu menüye ulaşmak istiyorsanız terminale şu komutu yazarak bütün parametrelere ulaşabilirsiniz.

nmap –help

---

1) Basit Nmap taramaları

Burada sizlere en temel nmap sorgularını göstermeye çalışacağım.

a) Belirli Bir IP Adresini Taramak

nmap **<IP adresi>**

Hemen bir örnek ile gösterelim. “192.192.12.4” numaralı IP adresi için basit nmap sorgusu yazalım.

ÖRNEK: nmap 192.192.12.4

---

b) Birden Fazla IP Adreslerini Tarama

nmap **<IP adresi> <IP adresi>**

Hemen bir örnek ile gösterelim. “5.6.7.8” ve “5.6.7.9” numaralı IP adreslerini taramak için nmap sorgusu yazalım.

ÖRNEK: nmap 5.6.7.8 5.6.7.9

---

c) Belirli Bir Aralıktaki IP Adreslerini Tarama

nmap **<Network Range>**

Bulunduğunuz ağdaki tüm IP adreslerini taramak isteyebilirsiniz. Bunu yapmak oldukça kolaydır. Bulunduğunuz ağın subnet değeri yani range değerini girmeniz yeterlidir. Örnek olması için “5.5.5.0/24” değerine sahip bir ağı tarayalım.

ÖRNEK: nmap 5.5.5.0/24

---

d) Dosyada Yazılı Olan IP Adreslerini Tarama

nmap **-iL** <dosya ismi>

Bazen taramak istediğiniz IP adreslerinin bilgisi bir dosya içinde olabilir ya da birden fazla IP adresi taramak isteyebilirsiniz. Bu IP adreslerini bir dosya içine kaydederek tek bir nmap komutu ile bu IP adreslerini tek seferde tarayabilirsiniz. Dosya içinden okumamız sağlayan nmap parametresi **“-iL”** parametresidir. Örnek olması için mesela IP adreslerini “IP_add.txt” isimli bir dosyada tuttuğumu varsayalım. Buradaki IP adreslerini şu şekilde tarayabilirim.

ÖRNEK: nmap -iL IP_add.txt

---

e) Hostname Taraması

Bazen elinizde IP adresi olmayabilir. Bir web sitesini taramak isteyebilirsiniz. Ama bunu çalıştırmak günümüzde suç sayılabilir. O yüzden kurumsal web sitelerine nmap sorgusu yapmayınız.

nmap <web sitesi veya hostname>

Ben örnek olması için "abc.com" isimli siteye nmap sorgusu yapmak istersek aşağıdaki gibi yapabiliriz.

ÖRNEK: nmap abc.com

---

2) Port Taramaları ve Port Seçimleri

Basit nmap taramalarında taranan portlar genelde "TOP 100" yani en çok kullanılan 100 portu tarayarak yapılır. Ama günümüzde mevcut 65535 port bulunmaktadır. Hele ki bir CTF yarışmasında bütün portları taramanız gerekmektedir. Bunu yapmak için kullanacağımız parametre **"-p"** budur.

a) Tek Bir Portu Tarama

nmap **<IP Adresi>** -p **<port numarası>**

Bazen sadece bir port için bilgi toplamanız gerekebilir. Mesela HTTP servisi "80" numaralı portu kullanmaktadır. Sadece HTTP servisi hakkında bilgi toplamak istersek sadece "80" numaralı portu taramamız yeterlidir. Diğer portları taramaya gerek yoktur. IP adresi "5.5.5.9" olan bir sistemde sadce HTTP servisi hakkında bilgi almak istersek şu şekilde yapmamız gerekmektedir.

ÖRNEK: nmap 5.5.5.9 -p 80

---

b) Belirli Aralıktaki IP Adreslerini Tarama

nmap **<IP Adresi>** -p **<port aralığı>**

Hemen 500 ve 1300 arasındaki portları tarayalım.

ÖRNEK: nmap 5.5.5.9 -p 500–1300

---

c) Bütün Portları Taramak

CTF yarışmalarında veya pentest çalışmalarında bütün portları taramamız gerekmektedir. Bunun için sadece parametre olarak "-p-" yazmanız yeterlidir.

nmap **<IP Adresi> -p-**

Hemen bir örnek yapalım. "5.5.5.6" numaralı IP adresindeki tüm portları tarayalım.

ÖRNEK: nmap 5.5.5.6 -p-

---

d) 100 Popüler Portu Hızlı Bir Şekilde Taramak

Bunu yapmak için tek bir parametre yeterlidir. “-F” parametresi ile bunu hızlıca yapabilirsiniz.

```
nmap -F <IP adresi>
```

Hemen bir örnekte gösterelim.

ÖRNEK: nmap -F 5.5.5.6

---

e) UDP Portlarını Taramak

```
nmap -sU <IP Adresi>
```

Bazen sadece UDP bağlantısı kullanan portları tespit etmek isteyebiliriz. Bütün portlar üzerinde UDP bağlantısı kullanan portları tespit etmek için aşağıdaki örnek size yardımcı olucaktır.

ÖRNEK: nmap -sU -p- 5.5.6.7

---

f) TCP Bağlantısı Taraması

Sadece TCP bağlantısı kullanan portları kullanan portları tespit etmek için;

```
nmap -sT <IP adresi>
```

Hemen bir örnekte gösterelim.

ÖRNEK: nmap -sT 4.4.4.9

---

g) TCP SYN Scan

TCP SYN scan default olarak kullanılan bir taramadır. Siz bunu parametre olarak vermeseniz bile nmap bunu kendi otomatik olarak kullanacaktır.

```
nmap -sS <IP adresi>
```

---

3) Servisler Ve İşletim Sistemi Sistemi Hakkında Bilgi Toplama

Bu bölüm oldukça büyük önem taşımaktadır. Genelde bir sisteme nasıl sızabileceğiniz hakkında en büyük bilgiyi bu aşamada öğrenirsiniz.

a) Servisleri Tespit Etme

```
nmap -sV <IP Adresi>
```

Yukarıdaki genel gösterimde “-sV” parametresi bize servisleri tespit etmemizde bize yardımcı olur. Hemen bir örnek ile görelim

ÖRNEK: nmap -sV 5.5.5.3

Ama tabiki de bu işlemi daha agresif yapmamızı sağlayan yardımcı bir parametre bulunmaktadır. Bunun kullanımı da aşağıdaki gibidir.

nmap -sV –version-intensity <Intensity Değeri 0–9 arasında> <IP adresi>

“ –version-intensity” paremetrisi ile versiyon tespitini daha agresif şekilde yapabiliriz. Intensity değeri ise “0–9” arasında bir değer almaktadır. Hemen bir örnek ile görelim.

ÖRNEK: nmap -sV -a-version-intensity 7 143.156.7.94

---

b) İşletim Sistemini Tespit Etme

nmap -O <IP adresi>

“-O” parametresi ile işletim sistemini tespit edebiliriz. Hemen bir örnekte görelim.

ÖRNEK: nmap -O 56.36.78.3

---

c) Karma Tarama

Nmap üzerinde tek bir parametre ile hem servisler hem de işletim sistemi hakkında tarama yapabiliriz.

nmap -A <IP adresi>

“-A” parametresi güzel bir parametredir. Ben de genelde bu parametreyi kullanılırım. İki işi aynı anda yapmak her zaman daha iyidir.

ÖRNEK: nmap -A 5.5.56.67

---

d) PING Atmadan Tarama Yapma

Karşı tarafa ping atmadan nmap taraması yapmak için “-PN” parametresi kullanılır.

nmap -PN <IP adresi>

---

4) Nmap Çıktılarını Kaydetme

Tarama sonucu elde ettiğiniz bilgileri bir yere kaydetmeniz gerekebilir. Bunun için kullanacağınız birkaç parametre bulunmaktadır.

a) Dosyayı Normal Kaydetme

nmap -oN <Dosya ismi> <IP adresi>

Mesela ben nmap sonucumu “sonuc.txt” dosyasına kaydedeyim.

ÖRNEK: nmap -oN sonuc.txt 192.168.10.7

---

b) XML Dosyası Olarak Kaydetme

nmap -oX <Dosya ismi> <IP adresi>

Yukarıdaki örnekteki taramayı XML türünde kaydedelim.

ÖRNEK: nmap -oX sonuc.txt 192.168.10.7

---

c) Tüm Dosya Türlerinde Kaydetme

nmap -oA <Dosya ismi> <IP adresi>

“-oA” parametresi ile dosyaları tüm dosya türlerinde kaydedebiliriz. XML veya normal kaydetmenin birleştirilmiş hali düşünebilirsiniz.

ÖRNEK: nmap -oA sonuc.txt 192.168.10.7

---

5) Script Kullanma

Nmap bünyesinde 500 den fazla script barındırmaktadır. Bunları kullanarak daha fazla bilgi edinebilirsiniz. Bu scriptleri default olarak “-sC” parametresi ile kullanabilirsiniz.

nmap -sC <IP adresi>

Bir örnekte görelim.

ÖRNEK: nmap -sV -sC 192.168.10.7

Karma Örnekler

Arkadaşlar buraya kadar genelde parametreleri tek başına kullandık. Ama bu yanlış anlaşılmasın. Birden fazla parametre aynı anda kullanılabilir. Bunları aşağıdaki örnekte görebilirsiniz. “-T” parametresi hız ile ilgili bir parametredir.

1) nmap -p- -sV -sS 192.168.10.2

2) nmap -v -p 1–65535 -sV -O -sS -T5 192.168.10.2

3) nmap -v -sS -A -T5 192.168.10.2

4) nmap -sV -v -p 139,445 10.0.1.0/24

Buraya kadar olan her detayı en ince ayrıntısına kadar anlatmaya çalıştım. Herkesin kullanabileceği bir “cheet sheet” oluşturmayı denedim. Umarım sizler için faydalı olmuştur. Soru, görüş ve geri bildirimleriniz için **fatihturgutegitim@gmail.com** adresine mail atabilirsiniz.

Ayrıca bana linkedin üzerinden de ulaşabilirsiniz. Okuyan herkese teşekkür eder sağlıklı günler dilerim. Daha fazla bilgi edinmek isterseniz aşağıdaki linklere bakabilirsiniz. Bir sonraki yazımda görüşmek üzere…

Yararlı Linkler

1. https://highon.coffee/blog/nmap-cheat-sheet/
2. http://cs.lewisu.edu/~klumpra/camssem2015/nmapcheatsheet1.pdf
3. https://www.stationx.net/nmap-cheat-sheet/

Bunu paylaş:

- Twitter
- Facebook
-

Bunu beğen:

Beğen Yükleniyor...

İlgili

Fatih T. tarafından yayımlandı

Hacettepe Üniversitesi Bilgisayar mühendisliği öğrencisiyim. Siber güvenlik alanında yapmış olduğum çalışmaları sizlerle paylaşmaya çalışıyorum :) Tüm gönderileri Fatih T. ile görüntüle

29 Ağustos 2020

Cheet Sheet [TR], Write-Up

Yazı dolaşımı

Geçmişten Günümüze Siber Saldırılar
Kurum ve Şirketler için Siber Güvelik Çözümleri #1

Bir Cevap Yazın

Yorumunuzu buraya

Son Yazılar

- Active Directory Basics WriteUp – TryHackMe
- MAL: Strings WriteUp – TryHackMe
- CC: Pen Testing WriteUp – TryHackMe
- Linux “find” Komutu
- OWASP Top 10: Broken Access Control

Bizi Takip Edin

- Medium

- LinkedIn

Blogu E-posta ile Takip Et

Bu blogu takip etmek ve yeni gönderilerle ilgili bildirimleri e-postayla almak için e-posta adresinizi girin.

E-posta Adresi:

E-posta adresinizi girin

Takip Et

Yukarı ↑

%d blogcu bunu beğendi: