BiltekCyber

Nmap 101

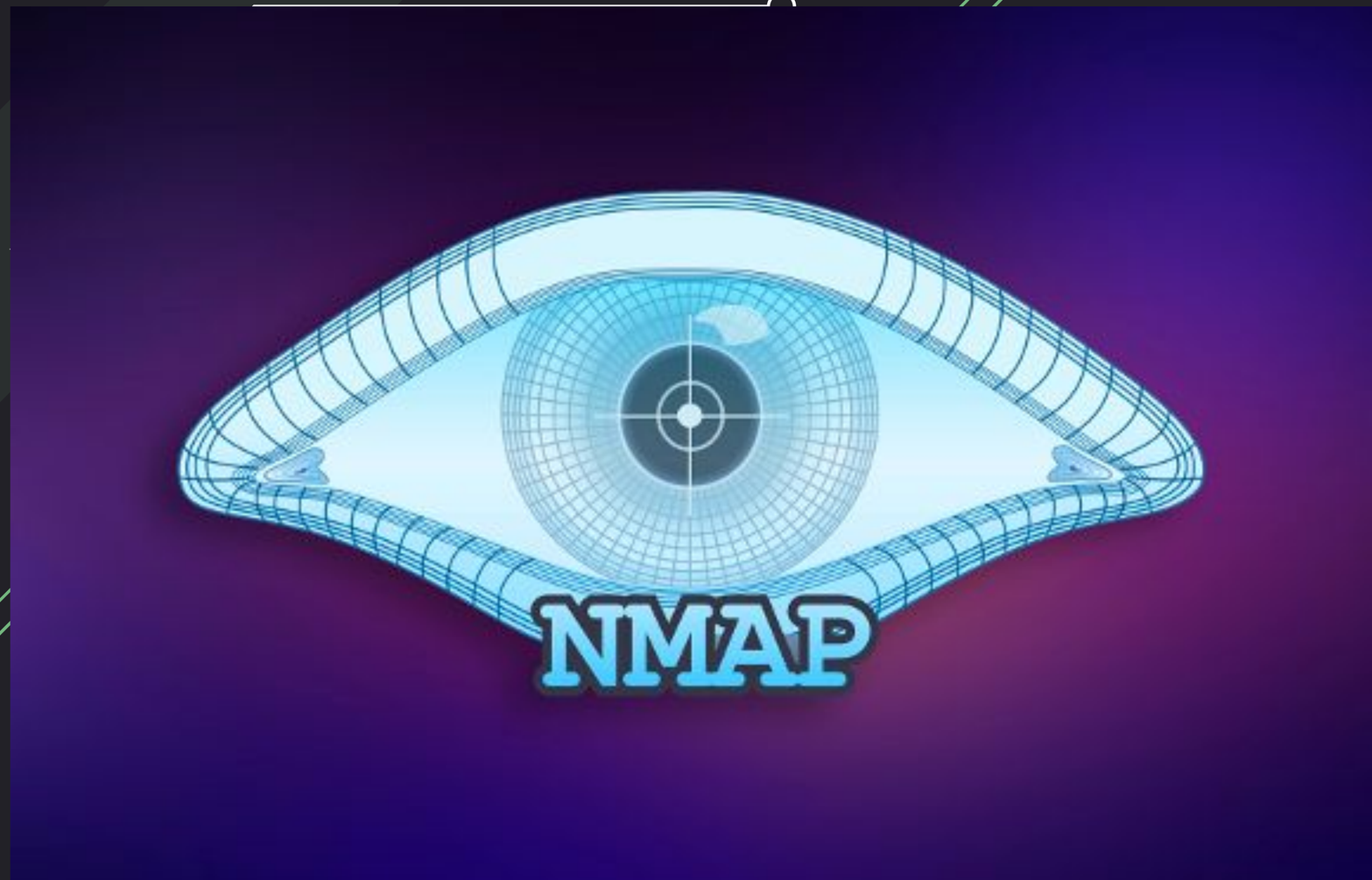
BiltekCyber

İçerik

BiltekCyber

Nmap Nedir?

Nmap (Network Mapper), açık kaynaklı bir ağ keşif ve güvenlik tarama aracıdır. Kali Linux gibi siber güvenlik ve penetrasyon testi odaklı işletim sistemlerinde yaygın olarak kullanılır. Nmap, ağlarda bulunan cihazları, açık portları, hizmetleri ve daha fazlasını tespit etmek için kullanılır.



BiltekCyber

Nmap Kullanımı

Nmap, güvenlik uzmanlarının ağları analiz etmek ve güvenlik açıklarını tespit etmek için güçlü bir araçtır. Ancak, etik kullanım ve yasal sınırlamalara dikkat edilmelidir. Nmap kullanımı için dikkat edilmesi gereken hususlar:

- Nmap gibi güvenlik araçları ağlarda tarama yaparken yasalara ve etik kurallara uygun olarak kullanılmalıdır. İzin almadan veya izinsiz olarak tarama yapmak yasa dışı olabilir.

- Tarama yapmadan önce hedef ağ veya cihaz sahiplerinden izin almalısınız. İzinsiz tarama, ağa gereksiz trafik yükü getirebilir ve hedef sistemleri kesintiye uğratabilir.

BiltekCyber

Nmap Kullanımı

- Yoğun taramalar ağ trafiğini artırabilir ve performans sorunlarına neden olabilir. Bu nedenle taramalar dikkatli bir şekilde planlanmalıdır.

- Hedef ağda güvenlik duvarları veya izinsiz giriş tespit/önleme sistemleri varsa, bu taramaları algılayabilir ve yanıltıcı sonuçlar üretebilir.

- Nmap taramaları, ağda bulunan cihazların ve servislerin güvenlik açıklarını belirlemek için kullanılır. Ancak bu taramalar, potansiyel olarak hedef cihazları ve ağı güvenlik riskine sokabilir.

BiltekCyber

Komutlar 101

BiltekCyber

Nmap Komutları

1-Temel Tarama Komutu:

Bu temel komut, belirtilen hedef IP adresini varsayılan port taraması yaparak analiz eder.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap target_ip
```

2-Belirli Portları Tarama:

Sadece belirli portları taramak için -p parametresini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -p 80,443 target_ip
```

Nmap Komutları

3-Ağ Aralığı Tarama:

Bir ağ aralığını taramak için CIDR gösterimini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap 192.168.1.0/24
```

4-Servis Algılama:

Çalışan servisleri algılamak için -sV parametresini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -sV target_ip
```

Nmap Komutları

5-İşletim Sistemi Algılama:

Hedefin işletim sistemini tahmin etmek için -O parametresini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -O target_ip
```

6-Hızlı Tarama:

Hızlı sonuçlar elde etmek için -F parametresini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -F target_ip
```

Nmap Komutları

7-Hedefteki Tüm Hostları Gösterme:

Bir ağdaki tüm aktif cihazları listelemek için -sn parametresini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -sn 192.168.1.0/24
```

8-TCP SYN Taraması:

TCP SYN taraması, açık portları hızlı bir şekilde tespit etmek için kullanılır.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -sS target_ip
```

Nmap Komutları

9-UDP Taraması:

UDP portlarını taramak için -sU parametresini kullanabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap -sU target_ip
```

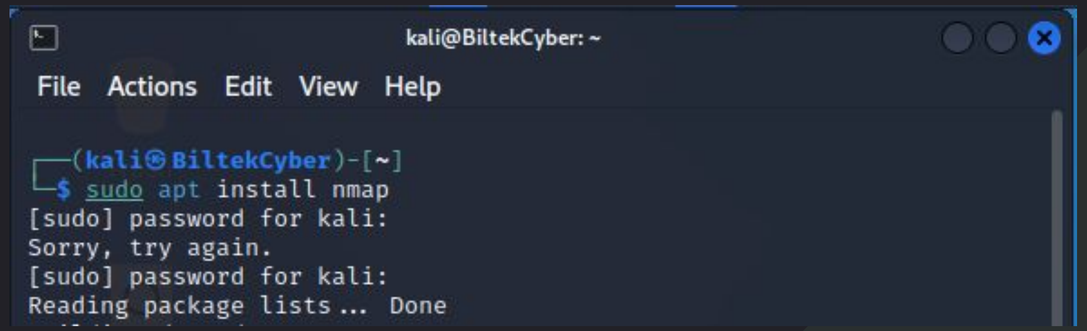
10-Betik Taraması:

NSE (Nmap Scripting Engine) ile özel betik taraması yapabilirsiniz.

```
┌──(kali㉿BiltekCyber)-[~]
└─$ nmap --script script_name target_ip
```

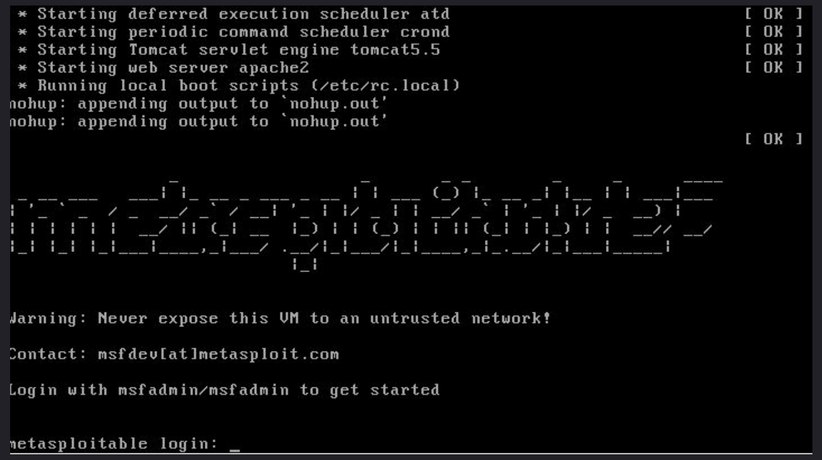
BiltekCyber

Nmap Kurulumu



Nmap aracının kurulumu için ilk olarak yapmamız gereken ‘sudo apt install nmap’ komutunu kullanarak araca ait dosyaların yüklenmesini sağlayalım.

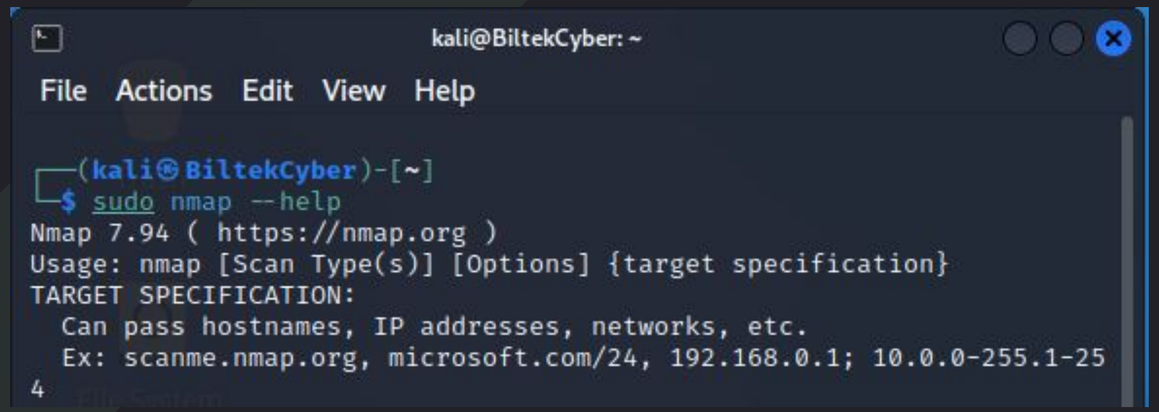
Not: Bu eğitim içeriğimizde nmap aracını kullanmak için kendi kurmuş olduğumuz metasploitable 2 zafiyetli makine kullanılmaktadır



BiltekCyber

Nmap Kullanımı

Nmap aracında kullanabileceğiniz komutlar ve parametreler hakkında kısa bilgiler edinmek için ‘nmap –help’ parametresini kullanabilirsiniz.



BiltekCyber

Nmap Kullanımı

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ setkbmap tr
-bash: setkbmap: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9c:56:4e
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9c:564e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5682 (5.5 KB)  TX bytes:8368 (8.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29705 (29.0 KB)  TX bytes:29705 (29.0 KB)

msfadmin@metasploitable:~$ _
```

İlk olarak zafiyetli makinenin ip adresini öğrenelim ve ardından nmap aracını kullanarak cihaz hakkında hangi bilgileri elde edebileceğimize bakalım.

Ekran görüntüsünde belirtildiği üzere ip adresimiz 10.0.2.6

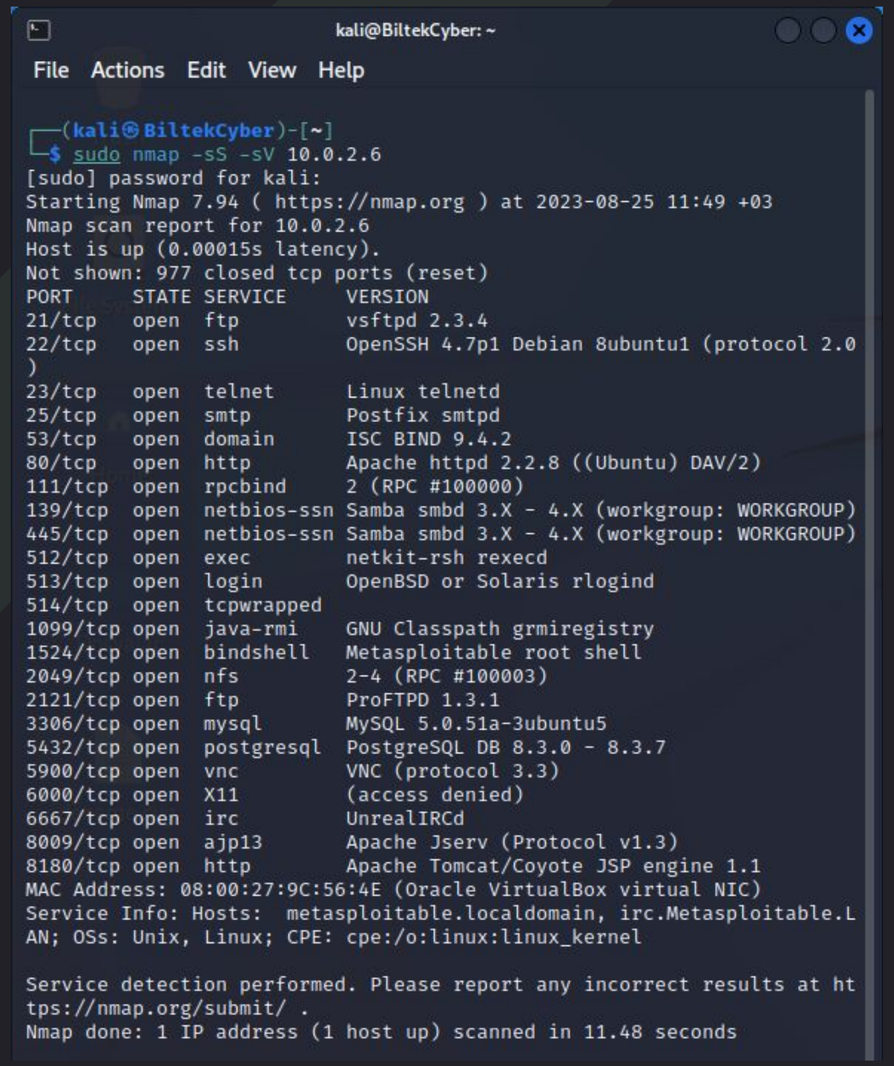
BiltekCyber

Nmap Kullanımı

‘sudo’ komutunu kullanarak root kullanıcısının yetkisiyle elde edeceğimiz sonuçlar yandaki görselde verilmiştir.

‘-sS, -sV’ parametrelini kullandığımız bu örnekte hangi portların açık olduğunu, servislerin durumunu ve isimlerini rahatlıkla görüntüleyebiliyoruz.

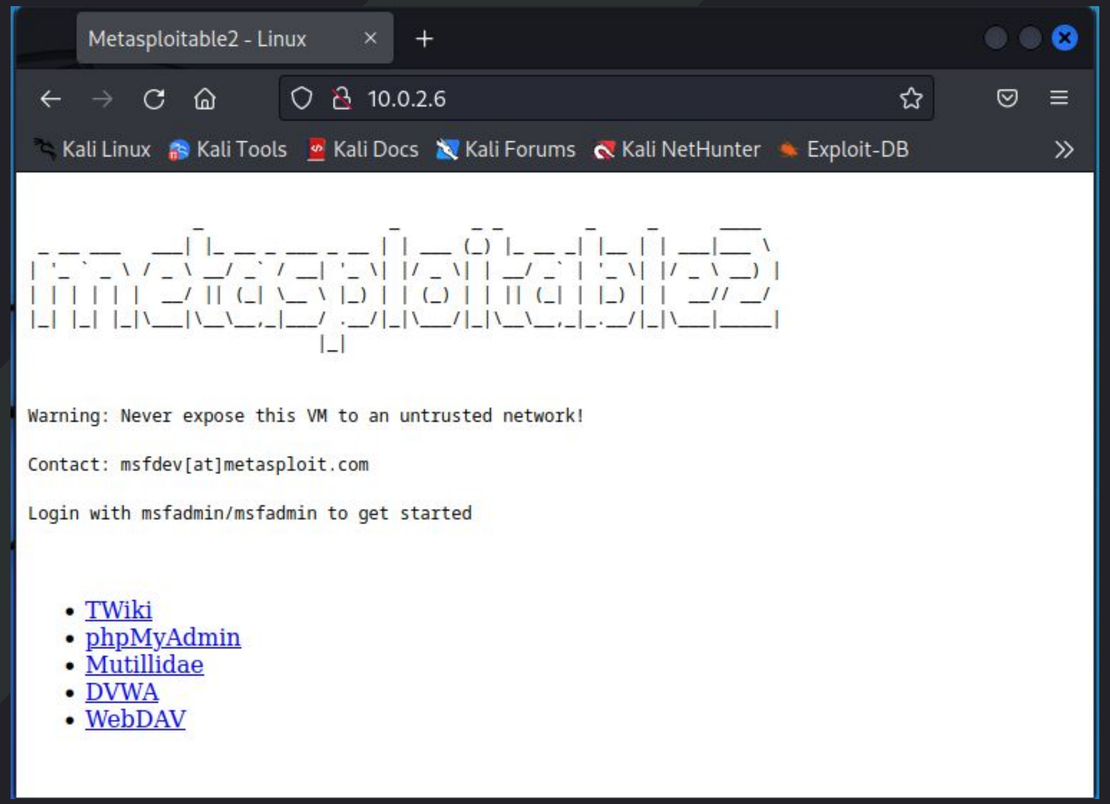
Örneğin 80 numaralı portta bir http server çalıştığı belirtilmiş.



BiltekCyber

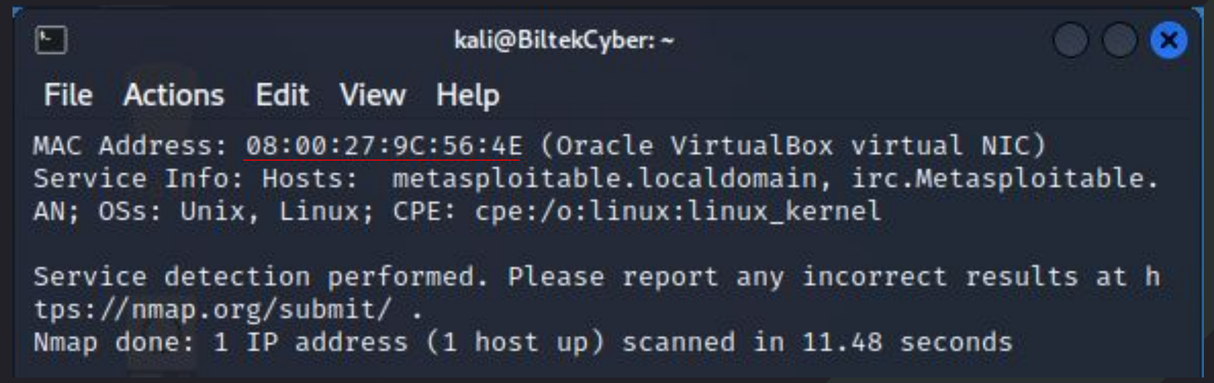
Nmap Kullanımı

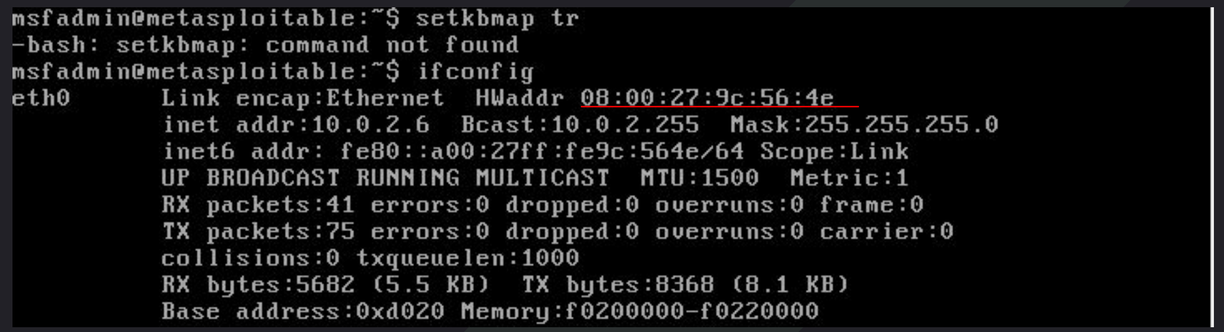
Önceden belirttiğimiz http adresine giriş yaparak website açığına kolaylıkla erişebiliriz.



BiltekCyber

Nmap Kullanımı





Bunların dışında çıktının aşağısında cihazın MAC adres bilgilerini, makinede çalışır durumda olan host isimlerini de görebilirsiniz.

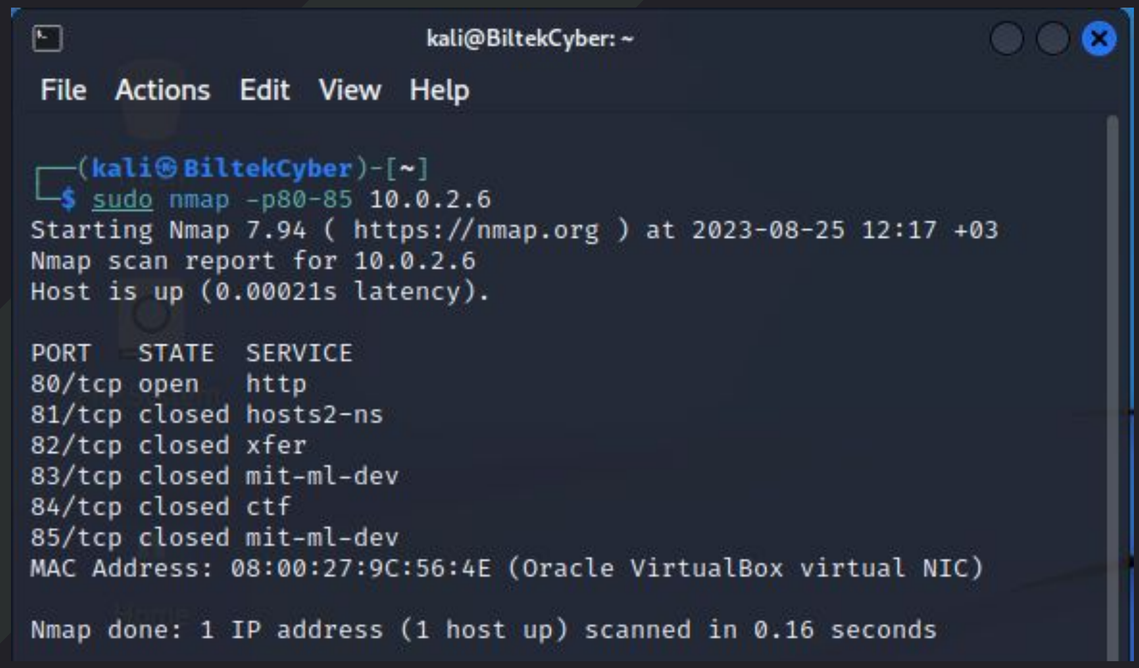
Yanda zafiyetle makineye ait MAC adresi bilgisinin Kali Linux makinesiyle tamamen uyuştuğunu görebilirsiniz.

BiltekCyber

Nmap Kullanımı

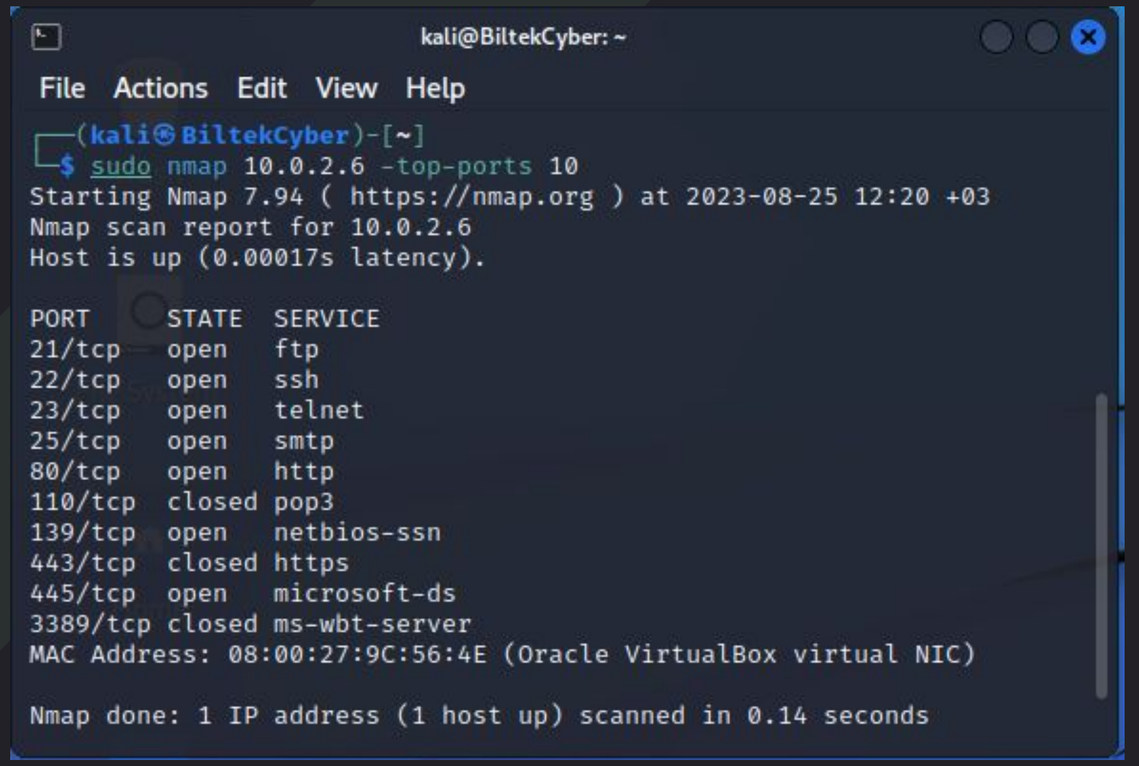
Eğer bütün portları taramak yerine belirli bir portun taranmasını istiyorsanız ‘-p’ parametresinin hemen ardından istediğiniz portu belirterek sadece o portun veya portların taranmasını sağlayabilirsiniz.

Yandaki örnekte 80-85 port aralığı taranmış olup sadece 80 numaralı portun açık olduğu görülmektedir.



Nmap Kullanımı

Aynı zamanda ‘-top-ports’ parametresinin sayesinde en çok kullanılan portların taranmasını ve durumlarının listelenmesini sağlayabilirsiniz.



BiltekCyber

Kaynakça

1-https://nmap.org/book/man-briefoptions.html
2-https://nmap.org/book/
3-https://nmap.org/book/nse.html
4-https://tr.wikipedia.org/wiki/Nmap
5-https://sudo.ubuntu-tr.net/nmap-komutu-ve-kullanimi

BiltekCyber

Hazırlayan

Adı: Yahya
Soyadı: Çakıcı
Fakülte: Mühendislik ve Doğa Bilimleri Fakültesi
Departman: Yazılım Mühendisliği 2.Sınıf

Linkedin: https://www.linkedin.com/in/yahya-çakıcı-584004256/