

# Nmap 101



# İçerik

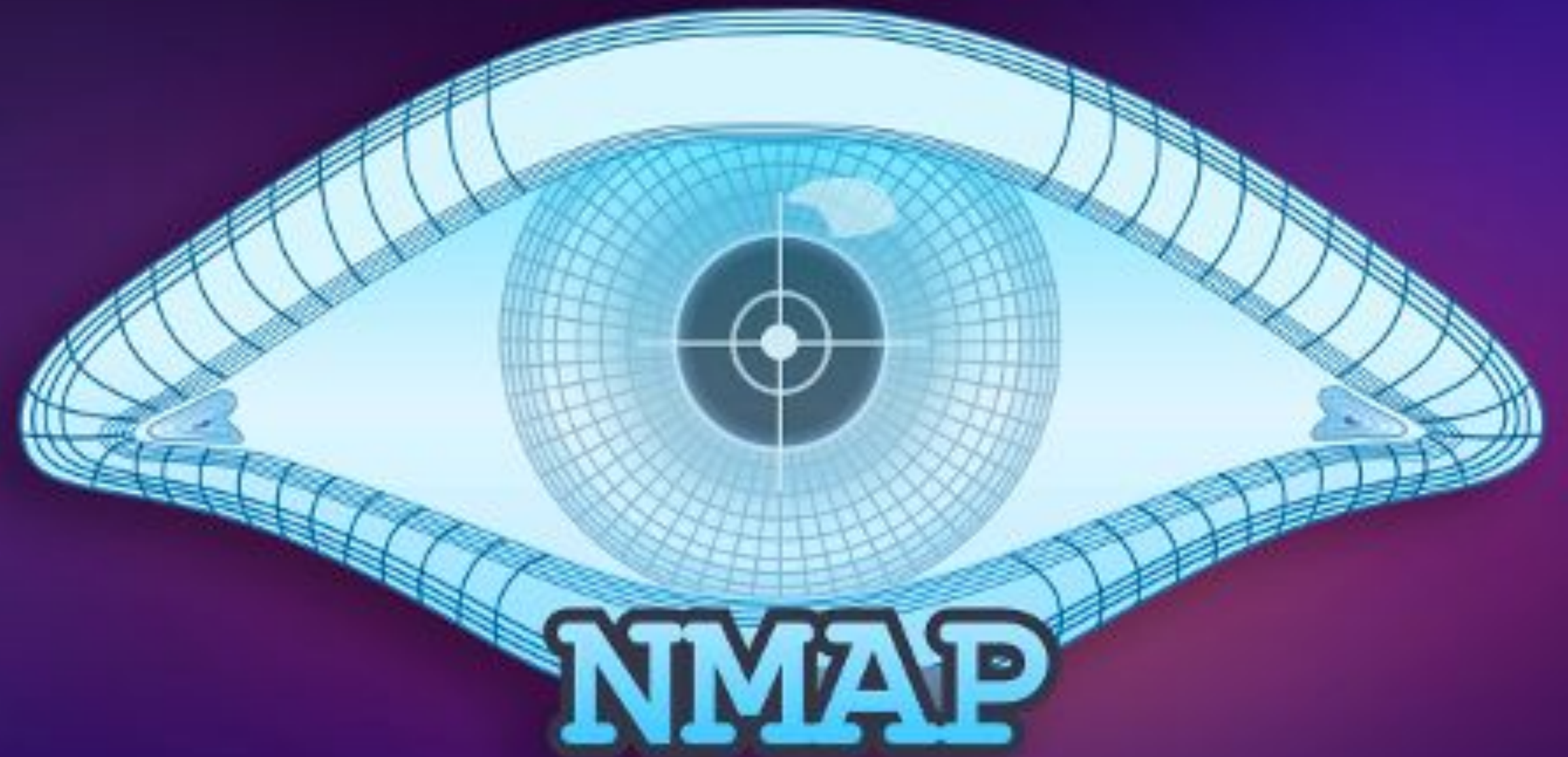
Nmap 101	01
Nmap Nedir?	03
Komutlar 101	06
Nmap Kullanımı	12





# 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.





# 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.







# 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



# 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
```





# Nmap Kurulumu

```
kali@BiltekCyber: ~  
File Actions Edit View Help  
  
(kali@BiltekCyber)-[~]  
$ sudo apt install nmap  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Reading package lists... Done
```

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

```
* Starting deferred execution scheduler atd [ OK ]  
* Starting periodic command scheduler cron [ OK ]  
* Starting Tomcat servlet engine tomcat5.5 [ OK ]  
* Starting web server apache2 [ OK ]  
* Running local boot scripts (/etc/rc.local)  
nohup: appending output to 'nohup.out'  
nohup: appending output to 'nohup.out' [ OK ]  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: _
```



# Nmap Kullanımı

Nmap aracında kullanabileceğiniz komutlar ve parametreler hakkında kısa bilgiler edinmek için 'nmap --help' parametresini kullanabilirsiniz.

```
kali@BiltekCyber: ~  
File Actions Edit View Help  
  
(kali@BiltekCyber)-[~]  
$ sudo nmap --help  
Nmap 7.94 ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-25  
4
```







# 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







# 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.

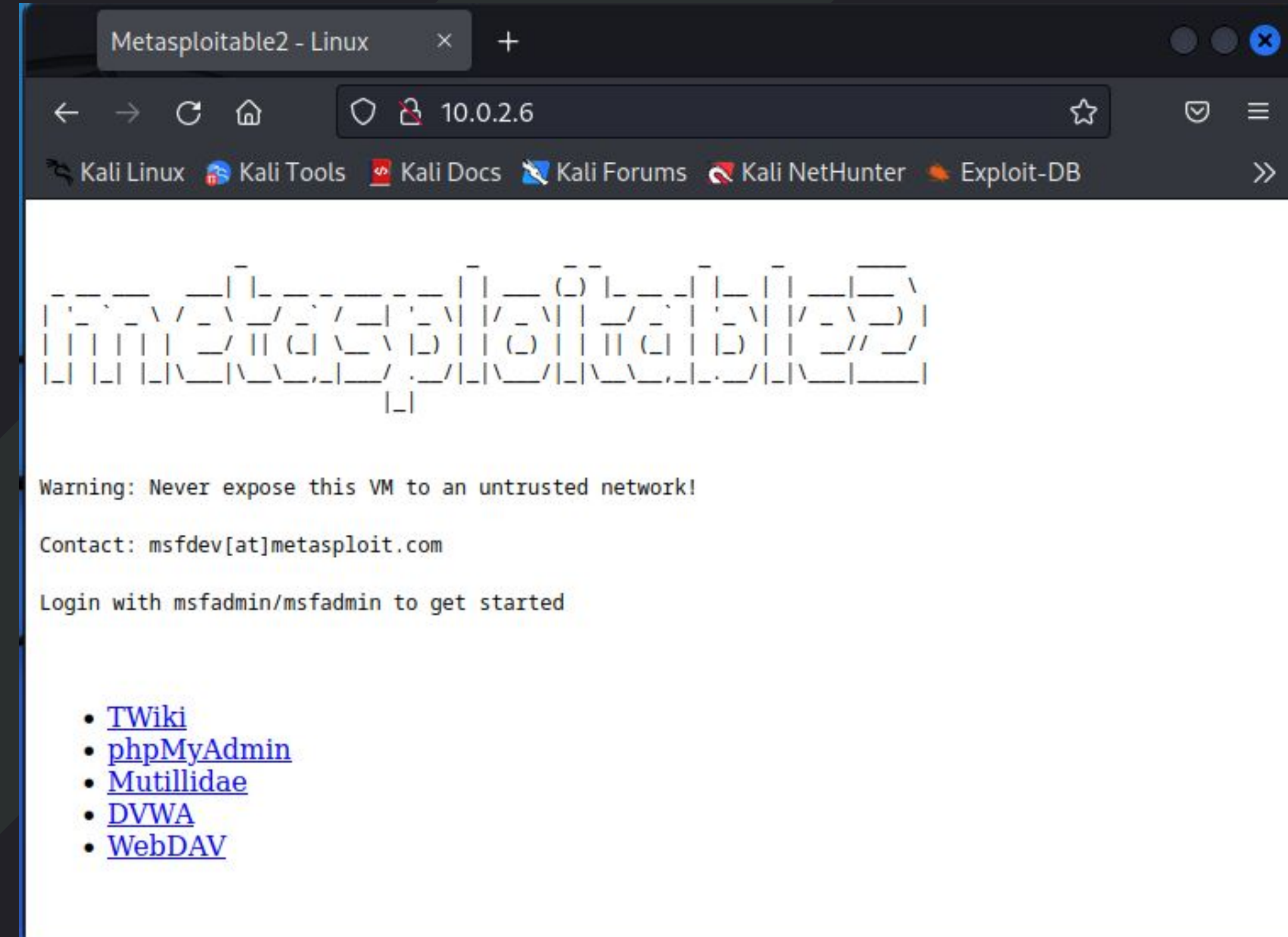
```
kali@BiltekCyber: ~  
File Actions Edit View Help  
  
(kali@BiltekCyber)-[~]  
$ sudo nmap -sS -sV 10.0.2.6  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 11:49 +03  
Nmap scan report for 10.0.2.6  
Host is up (0.00015s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:9C:56:4E (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.L  
AN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```





# Nmap Kullanımı

Önceden belirttiğimiz http adresine giriş yaparak website açığına kolaylıkla erişebiliriz.





# Nmap Kullanımı

```
kali@BiltekCyber: ~  
File Actions Edit View Help  
MAC Address: 08:00:27:9C:56:4E (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.  
AN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at h  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```

```
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
```

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.







# 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.

```
kali@BiltekCyber: ~  
File Actions Edit View Help  
  
(kali@BiltekCyber)-[~]  
$ sudo nmap -p80-85 10.0.2.6  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 12:17 +03  
Nmap scan report for 10.0.2.6  
Host is up (0.00021s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
81/tcp    closed hosts2-ns  
82/tcp    closed xfer  
83/tcp    closed mit-ml-dev  
84/tcp    closed ctf  
85/tcp    closed mit-ml-dev  
MAC Address: 08:00:27:9C:56:4E (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```





# Nmap Kullanımı

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

```
kali@BiltekCyber: ~  
File Actions Edit View Help  
(kali@BiltekCyber)-[~]  
$ sudo nmap 10.0.2.6 -top-ports 10  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 12:20 +03  
Nmap scan report for 10.0.2.6  
Host is up (0.00017s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
80/tcp    open  http  
110/tcp   closed pop3  
139/tcp   open  netbios-ssn  
443/tcp   closed https  
445/tcp   open  microsoft-ds  
3389/tcp  closed ms-wbt-server  
MAC Address: 08:00:27:9C:56:4E (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```





# 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/>

