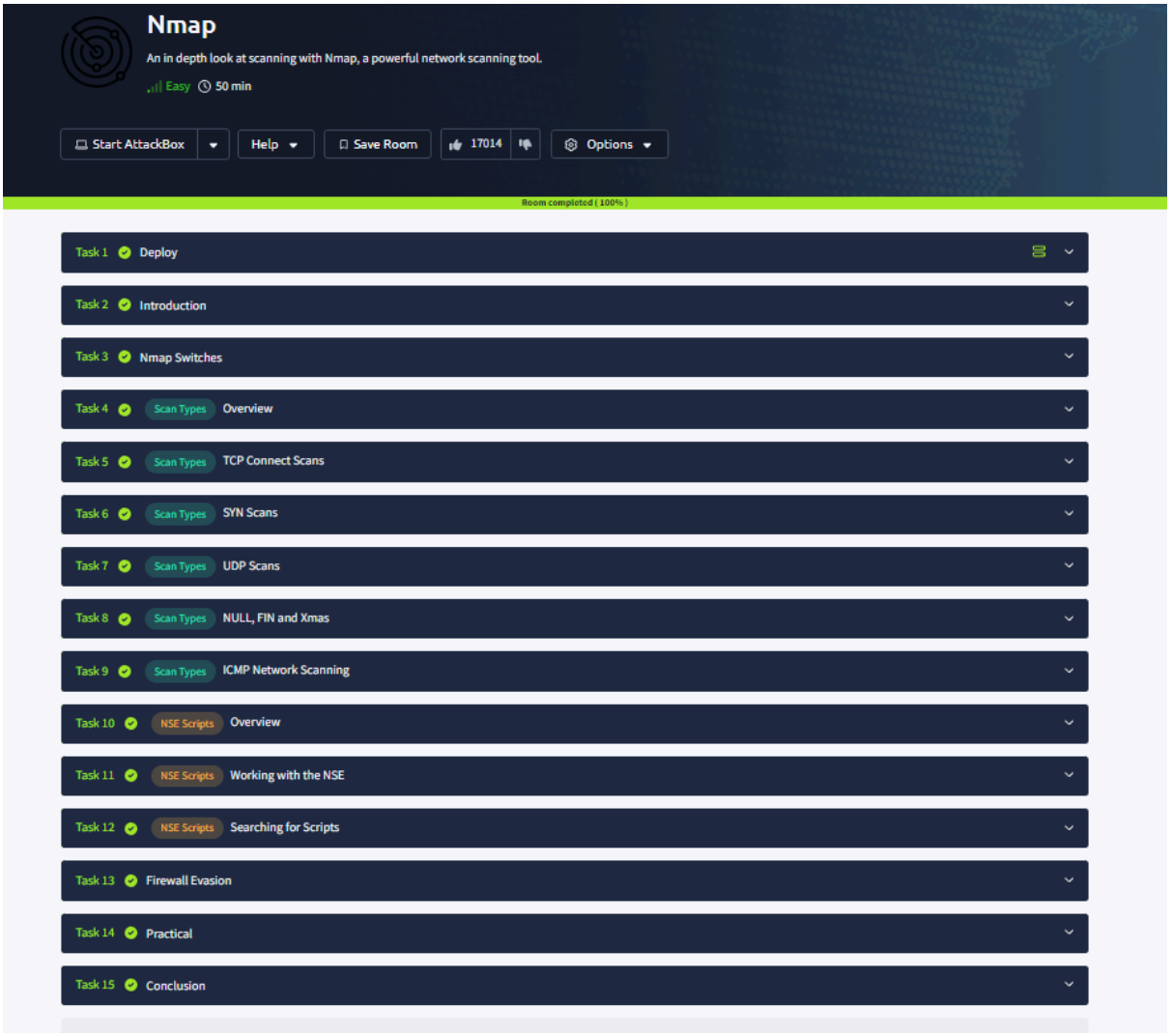
Nmap



1. How many tcp ports are open on the box? What command did you use?
   Your response: 23

2. How many udp ports are open on the box? What command did you use?
   Your response: 0

3. What is the version of ftp?
   Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV -p 21 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:09 EDT
Nmap scan report for 10.13.1.36
Host is up (0.038s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix
```

4. What is the version of ssh?
   Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV -p 22 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:11 EDT
Nmap scan report for 10.13.1.36
Host is up (0.041s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

5. What is the version of Apache?
   Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV -p 80,443 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:13 EDT
Nmap scan report for 10.13.1.36
Host is up (0.038s latency).

PORT    STATE  SERVICE VERSION
80/tcp  open   http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp closed https
```

6. Is anonymous ftp access allowed on the box? What command did you use? (Use only nmap)
   Your response: yes

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --script ftp-anon -p 21 10.13.1.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 10:15 EDT
Nmap scan report for 10.13.1.36
Host is up (0.14s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

7. Do a SYN scan. Which command did you use?
   Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ sudo nmap -sS 10.13.1.36 | wc -l
30
```

8. Do a scan that bypasses a firewall. What command did you use?
   Your response
   - nmap -sT 10.13.1.36 **#WORKED**
   - Sudo nmap -sI zombie_ip 10.13.1.36 **#BLOCKED**
   - Sudo nmap -f 10.13.1.36 **#FILTERED**
   - Sudo nmap -sS -Pn -D decoy1,decoy2,your_ip 10.13.1.36 **#WORKED**
   - nmap -r 10.13.1.36 **#WORKED**
9. Run a scan with the default NSE scripts. Which flag do you use?
   Your response:

   -sC
10. What service occupies port 8180?
    Your response

```
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
```

11. What is the salt of the mysql service?
    Your response

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -p 3306 --script mysql-info 10.13.1.36
```

```
_  Salt: a)BRT/.:vh$wPf3i8{%B
```

12. What is the domain name ?
    Your response:

    nmap --script smb-os-discovery 10.13.1.36

    Gave the below responses

    localdomain
13. What is the FQDN of the box ?
    Your response

    metasploitable.localdomain
14. What is the os version ?
    Your response

    Unix
15. What is the version of Samba ?
    Your response

    3.0.20-Debian
16. Wat is the name of the box ?
    Your response

    Metasploitable

17. Do a scan on the subnet 10.xx.1.0/24. How many IP addresses respond? What command did you use? Charleroi : 10.11.0.1/24 Bruxelles : 10.12.0.1/24 Ghent : 10.13.0.1/24
    Your response

    Charleroi:

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sn 10.11.0.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 03:05 EDT
Nmap scan report for 10.11.0.1
Host is up (0.035s latency).
Nmap scan report for 10.11.0.126
Host is up (0.041s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.39 seconds
```

Bruxelles:

Ghent:

18. Do the same thing but with the top port option at 10. What command did you use?
    Your response:
    Scanning all 3 locations at once.

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap --top-ports 10 10.11.0.0/24 10.12.0.0/24 10.13.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 11:06 EDT
Nmap scan report for 10.11.0.1
Host is up (0.035s latency).
```