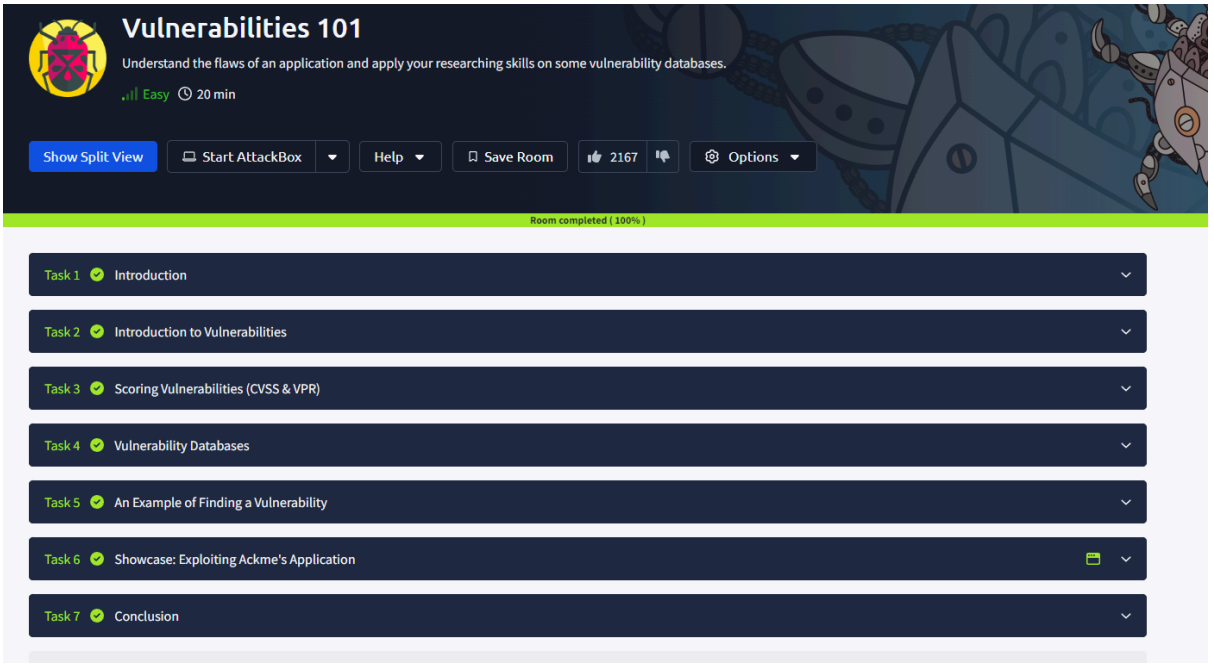
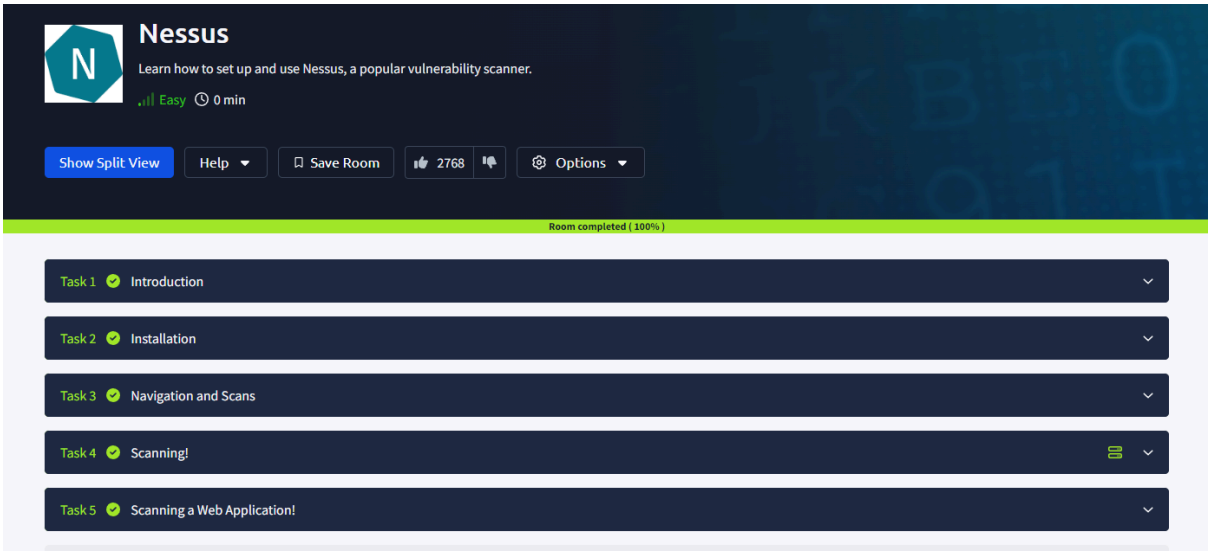
Vul_Scan:

1. Follow this room on try hack me

- https://tryhackme.com/room/vulnerabilities101



- https://tryhackme.com/room/rpnessusredux

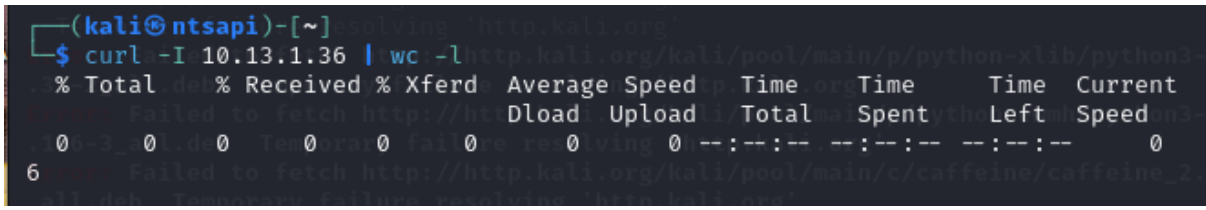


2. Questions :

2.1 Do a manual scan of the 10.13.1.36 box

- How many vulnerable services are there?

  6



- What are these services?

```
 program vers proto   port  service
  100000    2   tcp    111  portmapper
  100000    2   udp    111  portmapper
  100024    1   udp  38611  status
  100024    1   tcp  43460  status
  100003    2   udp   2049  nfs
  100003    3   udp   2049  nfs
  100003    4   udp   2049  nfs
  100021    1   udp  51045  nlockmgr
  100021    3   udp  51045  nlockmgr
  100021    4   udp  51045  nlockmgr
  100003    2   tcp   2049  nfs
  100003    3   tcp   2049  nfs
  100003    4   tcp   2049  nfs
  100021    1   tcp  53711  nlockmgr
  100021    3   tcp  53711  nlockmgr
  100021    4   tcp  53711  nlockmgr
  100005    1   udp  38923  mountd
  100005    1   tcp  48817  mountd
  100005    2   udp  38923  mountd
  100005    2   tcp  48817  mountd
  100005    3   udp  38923  mountd
  100005    3   tcp  48817  mountd
```

3. 2.2 Do a vulnerability scan with nmap.
    - How many vulnerabilities did nmap find ?
      32

```
┌──(kali㉿ntsapi)-[~]
└─$ nmap -sV 10.13.1.36 | wc -l
32
```

    - What are these services?

```
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?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry?
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?
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.82 seconds
```

4. 3.3 Do a vulnerability scan with Nessus.
    - How many vulnerabilities did nessus find ?
      After Launching Nessus and doing the setups.

- What are these services?