

Vul_Scan:

- Follow this room on try hack me
- <https://tryhackme.com/room/vulnerabilities101>

The screenshot shows the 'Vulnerabilities 101' room on TryHackMe. At the top, there's a yellow icon of a bug, the room title 'Vulnerabilities 101', a description 'Understand the flaws of an application and apply your researching skills on some vulnerability databases.', and a difficulty level 'All Easy' with a 20-minute duration. Below the title are several tabs: 'Show Split View', 'Start AttackBox', 'Help', 'Save Room', '2167', and 'Options'. A progress bar at the bottom indicates 'Room completed (100%)'. The main area contains a list of tasks, each with a green checkmark and a small gear icon: Task 1 (Introduction), Task 2 (Introduction to Vulnerabilities), Task 3 (Scoring Vulnerabilities (CVSS & VPR)), Task 4 (Vulnerability Databases), Task 5 (An Example of Finding a Vulnerability), Task 6 (Showcase: Exploiting Ackme's Application), and Task 7 (Conclusion).

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

The screenshot shows the 'Nessus' room on TryHackMe. It features a blue hexagonal icon with a white 'N', the room title 'Nessus', a description 'Learn how to set up and use Nessus, a popular vulnerability scanner.', and a difficulty level 'All Easy' with a 0-minute duration. The interface includes standard tabs like 'Show Split View', 'Help', 'Save Room', '2768', and 'Options'. A progress bar at the bottom shows 'Room completed (100%)'. The task list consists of five items: Task 1 (Introduction), Task 2 (Installation), Task 3 (Navigation and Scans), Task 4 (Scanning!), and Task 5 (Scanning a Web Application!).

2. Questions :

2.1 Do a manual scan of the 10.13.1.36 box

- How many vulnerable services are there?

6

A terminal window from Kali Linux showing the output of a curl command. The command is \$ curl -Ie 10.13.1.36 | wc -l. The output shows various HTTP headers and statistics. The last few lines of the output are:

```
$ curl -Ie 10.13.1.36 | wc -l
% Total    % Received   % Xferd  Average Speed   Time      Time     Current
          0          0        0      0.00K/s  0:00:00  0:00:00  0:00:00
          0          0        0      0.00K/s  0:00:00  0:00:00  0:00:00
```

- What are these services?

```

program vers proto port service
gn:100000 // 2 tcp 111 portmapper
gn:100000 // 2 udp 111 portmapper
gn:100024 // 1 udp 38611 status-roll
gn:100024 // 1 tcp 43460 status-roll
gn:100003 // 2 udp 2049 nfs
gn:100003 // 3 udp 2049 nfsali-roll
gn:100003 // 4 udp 2049 nfsali-roll
gn:100021 // 1 udp 51045 nlockmgr
gn:100021 // 3 udp 51045 nlockmgr
gn:100021 // 4 udp 51045 nlockmgr
gn:100003 // 2 tcp 2049 nfs
gn:100003 // 3 tcp 2049 nfs
gn:100003 // 4 tcp 2049 nfs
gn:100003 // 5 tcp 2049 nfs
gn:100021 // 1 tcp 53711 nlockmgr
gn:100021 // 3 tcp 53711 nlockmgr
gn:100021 // 4 TCP 53711 nlockmgr
gn:100005 // 1 udp 38923 mountd
gn:100005 // 1 TCP 48817 mountd
gn:100005 // 2 udp 38923 mountd
gn:100005 // 2 TCP 48817 mountd
gn:100005 // 3 udp 38923 mountd
gn:100005 // 4 TCP 48817 mountd
? 100005 3 tcp 48817 mountd

```

3. 2.2 Do a vulnerability scan with nmap.

- How many vulnerabilities did nmap find ?

32

```

└─(kali㉿ntapi)-[~] failure resolving host
$ nmap -sV --script=version 10.13.1.36 | wcat -l
32

```

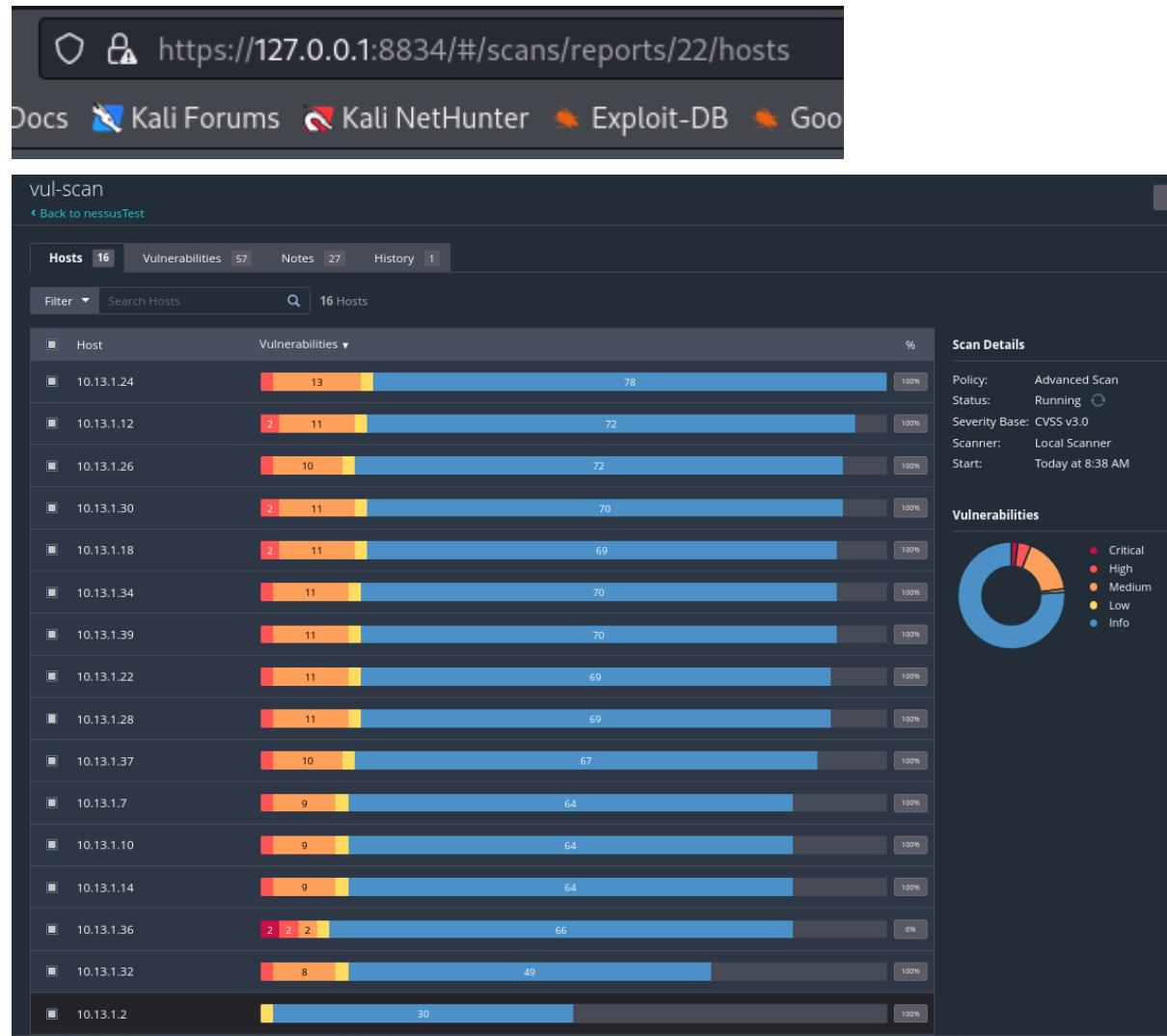
- What are these services?

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:linux: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?

