Scan run on Tryhackme Machine

```
root@ip-10-65-97-104:~# nmap -sV -sC -A 10.65.97.104
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-27 18:34 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with
--dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
--system-dns or specify valid servers with --dns-servers
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 22.22% done; ETC: 18:35 (0:00:11 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.89% done; ETC: 18:35 (0:00:04 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.74% done; ETC: 18:36 (0:00:00 remaining)
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.05% done; ETC: 18:37 (0:00:02 remaining)
Nmap scan report for 10.65.97.104
Host is up (0.000047s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
22/tcp   open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
53/tcp   open  domain       dnsmasq 2.90
| dns-nsid: 
|_  bind.version: dnsmasq-2.90
80/tcp   open  http         WebSockify Python/3.8.10
| fingerprint-strings: 
|   GetRequest: 
|     HTTP/1.1 405 Method Not Allowed
|     Server: WebSockify Python/3.8.10
|     Date: Thu, 27 Nov 2025 18:35:03 GMT
|     Connection: close
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 472
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 405</p>
|     <p>Message: Method Not Allowed.</p>
|     <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
|     </body>
|     </html>
|   HTTPOptions: 
```

```
|     HTTP/1.1 501 Unsupported method ('OPTIONS')
|     Server: WebSockify Python/3.8.10
|     Date: Thu, 27 Nov 2025 18:35:03 GMT
|     Connection: close
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 500
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 501</p>
|     <p>Message: Unsupported method ('OPTIONS').</p>
|     <p>Error code explanation: HTTPStatus.NOT_IMPLEMENTED - Server does not support this
operation.</p>
|     </body>
|_    </html>
|_http-server-header: WebSockify Python/3.8.10
|_http-title: Error response
81/tcp   open     http          Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
111/tcp  open     rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
389/tcp  open     ldap          OpenLDAP 2.2.X - 2.3.X
3389/tcp open     ms-wbt-server xrdp
5901/tcp open     vnc           VNC (protocol 3.8)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_vnc-info: ERROR: Script execution failed (use -d to debug)
6001/tcp open     X11           (access denied)
7777/tcp filtered cbt
7778/tcp filtered interwise
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=11/27%Time=692899D7%P=x86_64-pc-linux-gnu%r(Get
SF:Request,291,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nServer:\x2
SF:0WebSockify\x20Python/3\.8\.10\r\nDate:\x20Thu,\x2027\x20Nov\x202025\x2
SF:018:35:03\x20GMT\r\nConnection:\x20close\r\nContent-Type:\x20text/html;
SF:charset=utf-8\r\nContent-Length:\x20472\r\n\r\n<!DOCTYPE\x20HTML\x20PUB
SF:LIC\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20\"http://www\.w3\.org/TR/html4/strict\.dtd\">\n<html>\n\x20\x20\x
SF:20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"Con
SF:tent-Type\"\x20content=\"text/html;charset=utf-8\">\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20</head>
SF:\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Error\x20
SF:response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\x20405
SF:</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Method\x20Not\x20A
SF:llowed\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code\x20expla
SF:nation:\x20405\x20-\x20Specified\x20method\x20is\x20invalid\x20for\x20t
SF:his\x20resource\.</p>\n\x20\x20\x20\x20</body>\n</html>\n")%r(HTTPOptio
SF:ns,2B9,"HTTP/1\.1\x20501\x20Unsupported\x20method\x20\('OPTIONS'\)\r\nS
SF:erver:\x20WebSockify\x20Python/3\.8\.10\r\nDate:\x20Thu,\x2027\x20Nov\x
SF:202025\x2018:35:03\x20GMT\r\nConnection:\x20close\r\nContent-Type:\x20t
SF:ext/html;charset=utf-8\r\nContent-Length:\x20500\r\n\r\n<!DOCTYPE\x20HT
SF:ML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20\"http://www\.w3\.org/TR/html4/strict\.dtd\">\n<html>\n\
SF:x20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-eq
SF:uiv=\"Content-Type\"\x20content=\"text/html;charset=utf-8\">\n\x20\x20\
SF:x20\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x
SF:20</head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>
SF:Error\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20cod
SF:e:\x20501</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Unsupport
SF:ed\x20method\x20\('OPTIONS'\)\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p
SF:>Error\x20code\x20explanation:\x20HTTPStatus\.NOT_IMPLEMENTED\x20-\x20S
SF:erver\x20does\x20not\x20support\x20this\x20operation\.</p>\n\x20\x20\x2
SF:0\x20</body>\n</html>\n");
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.82 seconds
```

Reconnaissance

Nmap scan: nmap -sC -sV -A 10.65.97.104

Open Ports Found
Port

22	SSH	OpenSSH 8.2p1
53	DNS	dnsmasq 2.90
80	HTTP	WebSockify Python/3.8.10
81	HTTP	Apache 2.4.41
111	rbcbind	RPC
389	LDAP	OpenLDAP
3389	xRDP	Remote Desktop Protocol
5901	VNC	VNC protocol 3.8
6001	-	

Scan Overview

I performed an Nmap scan against the target host using the following command:

```
nmap -sV -sC -A 10.65.97.104
```

This scan enabled:

-sV : Version detection

-sC : Default NSE scripts

-A : OS detection, traceroute, advanced fingerprinting

The host was discovered to be up, with 989 ports closed and several key services running.

Open Ports & Services Identified

SSH – Port 22

Service: OpenSSH 8.2p1
Platform: Ubuntu Linux
SSH is available for remote login but requires authentication.

DNS – Port 53
Service: dnsmasq 2.90
The dnsmasq service is running and responds to DNS queries.

HTTP – Port 80
Service: WebSockify (Python/3.8.10)
Port 80 is running a WebSockify server, which responds to invalid HTTP methods with 405/501 error pages.
This does not appear to be the main web application.

HTTP – Port 81
Service: Apache/2.4.41 (Ubuntu)
This appears to be the primary web server, serving the default Apache page.
Further enumeration is likely needed here.

RPC Bind – Port 111
Service: rpcbind (versions 2–4)
The host exposes RPC services commonly used for NFS and other remote procedure calls.

LDAP – Port 389
Service: OpenLDAP 2.2.x – 2.3.x
LDAP is running and may allow anonymous queries (needs testing).

RDP – Port 3389
Service: xRDP
A remote desktop service is available, indicating the machine may support GUI access through RDP.

VNC – Port 5901
Service: VNC (protocol 3.8)
A VNC remote-access service is active.
Nmap couldn’t complete SSL info checks, but the service is visible.

X11 – Port 6001
Service: X11
The service is running but access denied, meaning remote GUI access might be partially restricted.

Filtered Ports
7777/tcp – cbt
7778/tcp – interwise
These ports are filtered, which means traffic is blocked or have been firewalled.

OS Fingerprinting

Nmap identified the target system as likely running a Linux 2.6.32 kernel.
This is an older kernel series and may have known vulnerabilities, though OS detection may not be perfect.

Summary of Findings

The target exposes a wide attack surface with multiple services running:

Two separate web servers (WebSockify on port 80, Apache on port 81)

SSH, DNS, RPC, LDAP

Remote desktop services (xRDP, VNC, X11)

For the Vulnversity room, the web server on port 81 is typically the entry point for further enumeration.