```
[]$ nmap -Pn -T4 -A -v 10.129.71.37
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http       Apache httpd 2.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.129.71.37/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3?
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap?
443/tcp   open  ssl/https?
|_ssl-date: 2020-12-28T17:34:45+00:00; +59m59s from scanner time.
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
4445/tcp  open  upnotifyp?
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: D9914F6343086F1A8FE996ED66283212
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: MiniServ/1.570
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Host: 127.0.0.1

dirbuster : https://10.129.71.37:443
choose wordlist eg :
/usr/share/dirbuster/wordlists/directory-list-1.0.txt

Apache, which is running on ports 80 and 443, will be the primary target

Exploit: ]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.129.71.37
The authenticity of host '10.129.71.37 (10.129.71.37)' can't be established.
RSA key fingerprint is SHA256:Ip2MswIVDX1AIEPoLiHsMFfdg1pEJ0XXD5nFEjki/hI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.71.37' (RSA) to the list of known hosts.
root@10.129.71.37's password:
Last login: Tue Sep 29 12:10:12 2020

Welcome to Elastix
----------------------------------------------------

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.129.71.37

[root@beep ~]# pwd
/root
[root@beep ~]# id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

```
[root@beep ~]# ls -a
.            .bash_profile             install.log.syslog
..           .bashrc             postnochroot
anaconda-ks.cfg  .cshrc                       root.txt
.bash_history      elastix-pr-2.2-1.i386.rpm  .tcshrc
.bash_logout       install.log               webmin-1.570-1.noarch.rpm

[root@beep ~]# cat root.txt
81ead442073e********************

[root@beep ~]# cd ..
[root@beep /]# ls
bin   dev  home  lost+found  mnt  proc          sbin  srv  tftpboot usr
boot  etc  lib  media              opt  root selinux  sys  tmp          var
[root@beep /]# cd home
[root@beep home]# ls
fanis  spamfilter
[root@beep home]# cd fanis
[root@beep fanis]# ls
user.txt

[root@beep fanis]# cat user.txt
7d7de30ff40b********************
[root@beep fanis]#
```