Ambassador

NMAP

```
nmap -sS -Pn 10.129.228.56
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 10:32 CET
Nmap scan report for 10.129.228.56
Host is up (0.060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
3306/tcp open  mysql
```

```
nmap -A 10.129.228.56
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 10:33 CET
Nmap scan report for 10.129.228.56
Host is up (0.043s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 29dd8ed7171e8e3090873cc651007c75 (RSA)
|   256 80a4c52e9ab1ecda276439a408973bef (ECDSA)
|_  256 f590ba7ded55cb7007f2bbc891931bf6 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: Hugo 0.94.2
|_http-title: Ambassador Development Server
3000/tcp open  ppp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie:
redirect_to=%2Fnice%2520ports%252C%2FTri%256Eity.txt%252ebak; Path=/;
HttpOnly; SameSite=Lax
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: deny
|     X-Xss-Protection: 1; mode=block
|     Date: Thu, 22 Dec 2022 09:34:00 GMT
|     Content-Length: 29
```

```
|     href="/login">Found</a>.
|   GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq,
TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: deny
|     X-Xss-Protection: 1; mode=block
|     Date: Thu, 22 Dec 2022 09:33:29 GMT
|     Content-Length: 29
|     href="/login">Found</a>.
|   HTTPOptions:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: deny
|     X-Xss-Protection: 1; mode=block
|     Date: Thu, 22 Dec 2022 09:33:34 GMT
|_    Content-Length: 0
3306/tcp open  mysql   MySQL 8.0.30-0ubuntu0.20.04.2
| mysql-info:
|   Protocol: 10
|   Version: 8.0.30-0ubuntu0.20.04.2
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: FoundRows, InteractiveClient,
IgnoreSpaceBeforeParenthesis, SupportsTransactions, Support41Auth,
Speaks41ProtocolOld, LongColumnFlag, IgnoreSigpipes,
SwitchToSSLAfterHandshake, SupportsLoadDataLocal, ODBCClient,
Speaks41ProtocolNew, ConnectWithDatabase, LongPassword, SupportsCompression,
DontAllowDatabaseTableColumn, SupportsAuthPlugins,
SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: <,miU\x0F\x07\x073\x03\x0F(:\x15\x10\x08fAJJ
|_  Auth Plugin Name: caching_sha2_password
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
```

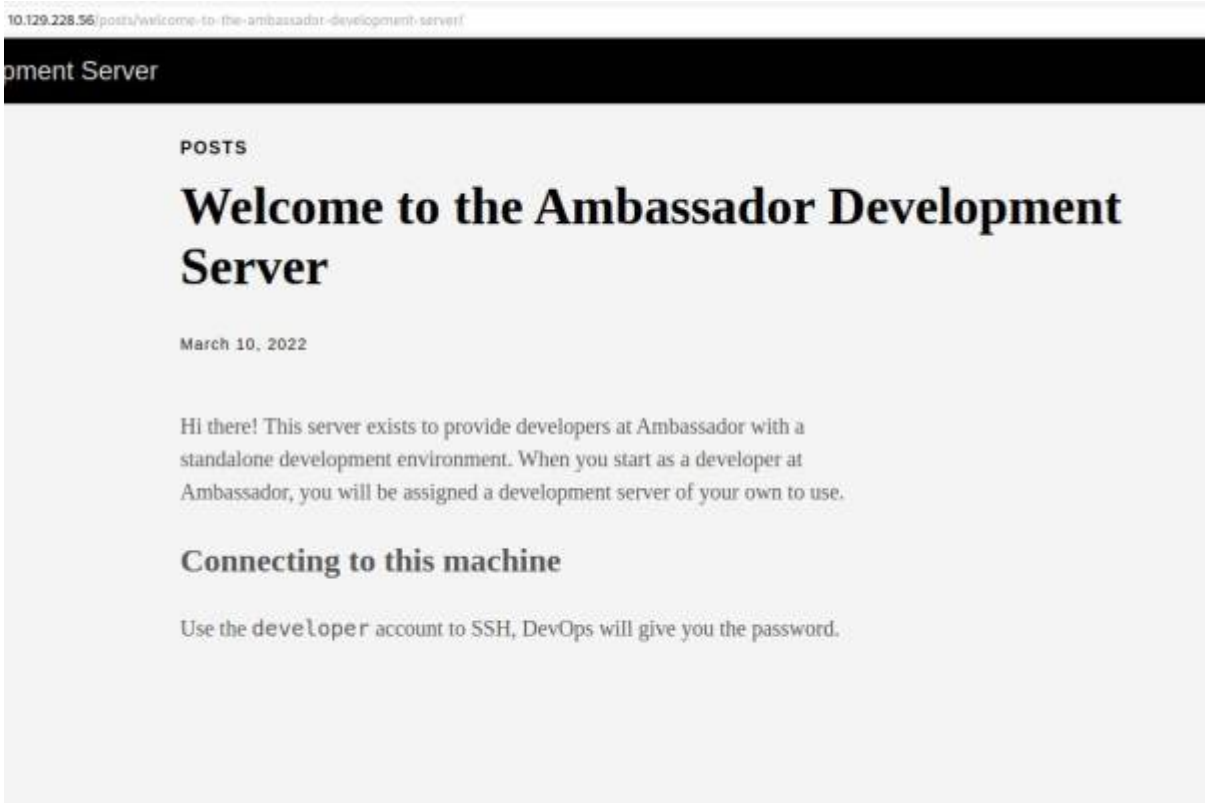
```
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.93%I=7%D=12/22%Time=63A4246A%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,174,"HTTP/1\.0\x20302\x20Found\r\nCache-Contr
SF:ol:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nExpi
SF:res:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache\r\nSet-Cookie:
SF:\x20redirect_to=%2F;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nX-Conte
SF:nt-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20deny\r\nX-Xss-Protec
SF:tion:\x201;\x20mode=block\r\nDate:\x20Thu,\x2022\x20Dec\x202022\x2009:3
SF:3:29\x20GMT\r\nContent-Length:\x2029\r\n\r\n<a\x20href=\"/login\">Found
SF:</a>\.\n\n")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(HTTPOptions,12E,"HTTP/1\.0\x20302\x20Found\r\nCa
SF:che-Control:\x20no-cache\r\nExpires:\x20-1\r\nLocation:\x20/login\r\nPr
SF:agma:\x20no-cache\r\nSet-Cookie:\x20redirect_to=%2F;\x20Path=/;\x20Http
SF:Only;\x20SameSite=Lax\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-
SF:Options:\x20deny\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20T
SF:hu,\x2022\x20Dec\x202022\x2009:33:34\x20GMT\r\nContent-Length:\x200\r\n
SF:\r\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-
SF:Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n40
SF:0\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x
SF:20close\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTTP/
SF:1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charse
SF:t=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TLSSes
SF:sionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text
SF:/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20R
SF:equest")%r(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(FourOhFourRequest,1A1,"HTTP/1\.0\x20302\x20Found
SF:\r\nCache-Control:\x20no-cache\r\nContent-Type:\x20text/html;\x20charse
SF:t=utf-8\r\nExpires:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache
SF:\r\nSet-Cookie:\x20redirect_to=%2Fnice%2520ports%252C%2FTri%256Eity\.tx
SF:t%252ebak;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nX-Content-Type-Op
SF:tions:\x20nosniff\r\nX-Frame-Options:\x20deny\r\nX-Xss-Protection:\x201
SF:;\x20mode=block\r\nDate:\x20Thu,\x2022\x20Dec\x202022\x2009:34:00\x20GM
SF:T\r\nContent-Length:\x2029\r\n\r\n<a\x20href=\"/login\">Found</a>\.\n\n
SF:");
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=12/22%OT=22%CT=1%CU=31938%PV=Y%DS=2%DC=T%G=Y%TM=63A424
OS:EA%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M539ST11NW7%O2=M539ST11NW7%O3=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST
OS:11NW7%O6=M539ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)EC
OS:N(R=Y%DF=Y%T=40%W=FAF0%O=M539NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G
OS:%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

```
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   41.91 ms 10.10.14.1
2   42.05 ms 10.129.228.56

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.52 seconds
```

Website



Gobuster

```
gobuster dir -w /usr/share/wordlists/dirb/common.txt --url
http://10.129.228.56
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.228.56
[+] Method:                  GET
[+] Threads:                 10
```

```
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2022/12/22 10:41:28 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/categories           (Status: 301) [Size: 319] [-->
http://10.129.228.56/categories/]
/images               (Status: 301) [Size: 315] [-->
http://10.129.228.56/images/]
/index.html           (Status: 200) [Size: 3654]
/posts                (Status: 301) [Size: 314] [-->
http://10.129.228.56/posts/]
/server-status        (Status: 403) [Size: 278]
/sitemap.xml          (Status: 200) [Size: 645]
/tags                 (Status: 301) [Size: 313] [-->
http://10.129.228.56/tags/]
Progress: 4561 / 4615
(98.83%)=============================================================
2022/12/22 10:41:49 Finished
===============================================================
```