Main Information

Information	Result
Organization	Unified Layer
Operating System	None
Country	United States
City	Provo
Hostnames	162-144-127-197.unifiedlayer.com

Scan info

Port: 443

Banner: HTTP/1.1 200 OK Date: Mon, 13 Sep 2021 05:55:08 GMT Server: Apache Last-Modified: Wed, 15 Jul 2020 19:10:22 GMT Accept-Ranges: bytes Content-Length: 41164 Content-Type: text/html

Port: 80

Banner: HTTP/1.1 302 Found Date: Mon, 13 Sep 2021 02:51:39 GMT Server: Apache Location: https://www.accurexmeasure.com/ Content-Length: 215 Content-Type: text/html; charset=iso-8859-1

Port: 123

Banner: NTP protocolversion: 3 stratum: 0 leap: 3 precision: -21 rootdelay: 0.0 rootdisp: 418.434585571 refid: 1229867348 reftime: 0.0 poll: 3

Port: 995

Banner: +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN .

Port: 993

Banner: * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed.

Port: 21

Banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 06:29. Server port: 21. 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 421 Can't change directory to /var/ftp/ [/] 211-Extensions supported: EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD AUTH TLS PBSZ PROT UTF8 TVFS ESTA PASV EPSV SPSV ESTP 211 End.

Port: 53

Banner: 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 Resolver name: server.accurexmeasure.com

Port: 22

Banner: SSH-2.0-OpenSSH_5.3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAxYJUSVgLaTgRGsZ9lBS4oROmtNOsE+uO7I3phWQbuH+pWy/c
iV0fMW+1+mcWsf2C0hRrEtYIMuHq9YkfLlBauy35xIz9xzzSy/RMSj0va7HbfzL1imR+IjA33tJN u4gnyv5/0/LtnpW8R1BmMS7W3pmPpFarNsKe4gZL/DQzWySmQubemOAARI91DQVK73wYXaRVD6/T
QZmejR1TGw9XE4kcd6CFrcmY3LTwQSSDxGwqJ/ctjgpTy4F3sWublmUV/u/VDR+Pj3SJvK8K+86z qMW/vwIMHR0WyOEcABWdQ1DjfUH1Rmp+Vx62LyltTwugS03YQSJRaAIxxinOUeoIow==
Fingerprint: de:54:2d:28:34:3b:c1:f2:b9:69:cf:92:c4:9d:d1:1f Kex Algorithms: diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1
diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc
cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160
hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com

Port: 53

Banner: 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 Resolver name: server.accurexmeasure.com

Port: 2082

Banner: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Sun, 05 Sep 2021 10:35:02 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: cpsession=%3aaSIVKnFNvPFP0HR1%2c615e8754e9f7300f83fae405d0c1b28d; HttpOnly; path=/; port=2082 Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: Horde=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2082 Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Set-Cookie: imp_key=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37296

Port: 2086

Banner: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Sat, 04 Sep 2021 00:36:41 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: whostmgrsession=%3aNY8I_viKI2g2fn11%2c2d5e835c556504f024735562d38a3e2f; HttpOnly; path=/; port=2086 Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: Horde=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2086 Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Set-Cookie: imp_key=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37291

Port: 465

Banner: 220-server.accurexmeasure.com ESMTP Exim 4.93 #2 Thu, 02 Sep 2021 00:58:43 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-server.accurexmeasure.com Hello 100.76.190.129 [100.76.190.129] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250 HELP

Port: 2087

Banner: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Tue, 31 Aug 2021 12:52:09 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: whostmgrsession=%3aQrqHQNihMVpkglYQ%2cef9ed9072557771fb35765cd46d536b1; HttpOnly; path=/; port=2087; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2087; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: imp_key=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 40362

Port: 26

Banner: 220-server.accurexmeasure.com ESMTP Exim 4.93 #2 Tue, 31 Aug 2021 09:51:30 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.

Port: 110

Banner: +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN .

Port: 143

Banner: * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed.

Port: 2083

Banner: HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Fri, 27 Aug 2021 12:33:22 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: cpsession=%3aAenjSxooFz2H42M7%2c2038931939c4e639716e80ffc2aaac78; HttpOnly; path=/; port=2083; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2083; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: imp_key=expired; HttpOnly; domain=162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.162.144.127.197; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 40367

Port: 3306

Banner: \x04Host \'129.161.17.254\' is not allowed to connect to this MySQL server

Port: 2080

Banner:

IP geolocation

Virustotal Information

Info	Results
Malicious	True
Malicious URLs	http://162.144.127.197/ https://162.144.127.197/ http://162.144.127.197:3786/ http://www.accurexmeasure.com/ http://accurex3d.accurexmeasure.com/ https://162.144.127.197:3786/ http://accurexmeasure.com/ http://accurexmeasure.com:443/ http://www.accurexmeasure.com/index.htm http://accurexmeasure.com/api/check.get https://www.accurexmeasure.com/upload/design/fonts/fonts/update/app/signin http://accurexmeasure.com/test1.js https://www.accurexmeasure.com/ https://accurexmeasure.com/
Domain Resolutions	accurex.co (2019-09-13 11:53:17) accurex3d.accurexmeasure.com (2019-11-05 23:26:56) accurex3d.com (2016-06-03 00:00:00) accurexmeasure.com (2019-12-12 06:17:25) bladeinspect.com (2019-11-29 10:24:07) ftp.tubemeasure.com (2021-02-07 23:02:27) m.accurexmeasure.com (2019-11-01 13:58:20) mail.accurex.co (2017-05-19 00:00:00) mail.accurexmeasure.com (2018-09-05 17:00:39) mail.bladeinspect.com (2020-04-27 19:53:17) mail.tubemeasure.com (2019-11-01 13:48:26) pop.tubemeasure.com (2021-02-08 07:45:10) smtp.tubemeasure.com (2021-02-07 23:57:23) tubemeasure.com (2019-11-04 20:17:36) webmail.tubemeasure.com (2021-02-08 20:47:09) www.accurex.co (2019-03-22 14:12:48) www.accurex3d.accurexmeasure.com (2019-11-05 00:57:25) www.accurexmeasure.com (2019-11-29 10:29:11) www.bladeinspect.com (2020-04-27 19:53:17) www.m.accurexmeasure.com (2019-11-04 16:43:18) www.mail.accurexmeasure.com (2019-10-03 04:22:07) www.tubemeasure.com (2019-11-04 20:17:36)

Download PDF Report
Return Home page