//EMMA JUNGER – 101292600

//SANIA RAFIQ JUDDHA – 101280650

//COMP3134

//ALL TASKS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

//Task 1

//> I begin by preforming an 'nslookup' cmd to reverse dns search the given domain.

//> nslookup lvclean.ca

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: lvclean.ca

Address: 50.87.146.7

//> Next I preform an 'nmap' search using the following scripts

//> -sC / Runs the default nmap scripts

//> -sV / Enumerate versions

//> I then pipe the appended output into this file

//> nmap -sC -sV 50.87.146.7 >> task1.txt

Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-24 14:27 UTC

Nmap scan report for 50-87-146-7.unifiedlayer.com (50.87.146.7)

Host is up (0.048s latency).

Not shown: 984 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Pure-FTPd

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

|\_ssl-date: 2022-01-24T14:28:13+00:00; 0s from scanner time.

22/tcp open ssh OpenSSH 5.3 (protocol 2.0)

| ssh-hostkey:

|\_ 1024 d5:5f:b5:05:51:e5:5b:98:6c:4c:10:2c:1c:c5:23:d2 (DSA)

25/tcp open smtp Exim smtpd 4.94.2

|\_smtp-commands: Couldn't establish connection on port 25

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

26/tcp open smtp Exim smtpd 4.94.2

|\_smtp-commands: Couldn't establish connection on port 26

53/tcp open domain ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)

| dns-nsid:

|\_ bind.version: 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6\_10.1

80/tcp open http Apache httpd

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: Apache

| http-title: 404 Error

|\_Requested resource was /404.html

|\_http-trane-info: Problem with XML parsing of /evox/about

110/tcp open pop3 Dovecot pop3d

|\_pop3-capabilities: PIPELINING RESP-CODES CAPA AUTH-RESP-CODE UIDL STLS USER SASL(PLAIN LOGIN) TOP

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

|\_ssl-date: 2022-01-24T14:28:13+00:00; 0s from scanner time.

143/tcp open imap Dovecot imapd

|\_imap-capabilities: IMAP4rev1 LOGIN-REFERRALS AUTH=PLAIN STARTTLS AUTH=LOGINA0001 IDLE listed NAMESPACE ID OK SASL-IR Pre-login more have post-login capabilities ENABLE LITERAL+

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

|\_ssl-date: 2022-01-24T14:28:14+00:00; 0s from scanner time.

443/tcp open ssl/http Apache httpd

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: Apache

| http-title: 404 Error

|\_Requested resource was /404.html

|\_http-trane-info: Problem with XML parsing of /evox/about

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

465/tcp open tcpwrapped

| smtp-commands: gator3003.hostgator.com Hello 50-87-146-7.unifiedlayer.com [159.89.118.73], SIZE 52428800, 8BITMIME, PIPELINING, PIPE\_CONNECT, AUTH PLAIN LOGIN, HELP,

|\_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

|\_ssl-date: 2022-01-24T14:28:12+00:00; 0s from scanner time.

587/tcp open tcpwrapped

| smtp-commands: gator3003.hostgator.com Hello 50-87-146-7.unifiedlayer.com [159.89.118.73], SIZE 52428800, 8BITMIME, PIPELINING, PIPE\_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP,

|\_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

993/tcp open ssl/imap Dovecot imapd

|\_imap-capabilities: IMAP4rev1 LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGINA0001 IDLE listed NAMESPACE ID OK LITERAL+ Pre-login more have post-login capabilities ENABLE SASL-IR

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

|\_ssl-date: 2022-01-24T14:28:12+00:00; 0s from scanner time.

995/tcp open ssl/pop3 Dovecot pop3d

|\_pop3-capabilities: CAPA PIPELINING AUTH-RESP-CODE RESP-CODES UIDL USER SASL(PLAIN LOGIN) TOP

| ssl-cert: Subject: commonName=\*.hostgator.com

| Subject Alternative Name: DNS:\*.hostgator.com, DNS:hostgator.com

| Not valid before: 2021-08-31T00:00:00

|\_Not valid after: 2022-08-31T23:59:59

|\_ssl-date: 2022-01-24T14:28:12+00:00; 0s from scanner time.

2222/tcp open ssh OpenSSH 5.3 (protocol 2.0)

| ssh-hostkey:

| 1024 d5:5f:b5:05:51:e5:5b:98:6c:4c:10:2c:1c:c5:23:d2 (DSA)

|\_ 2048 6e:d9:99:79:bd:f5:81:62:30:24:9e:58:6f:1f:c3:07 (RSA)

2525/tcp filtered ms-v-worlds

3306/tcp open mysql MySQL 5.6.41-84.1

| mysql-info:

| Protocol: 10

| Version: 5.6.41-84.1

| Thread ID: 30491985

| Capabilities flags: 65535

| Some Capabilities: SupportsTransactions, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, Support41Auth, IgnoreSigpipes, SupportsCompression, SwitchToSSLAfterHandshake, FoundRows, InteractiveClient, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, LongPassword, ConnectWithDatabase, LongColumnFlag, ODBCClient, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments

| Status: Autocommit

| Salt: ."^5+u27ZAsC2nVB)Ea8

|\_ Auth Plugin Name: mysql\_native\_password

Service Info: Host: gator3003.hostgator.com; OS: Linux; CPE: cpe:/o:redhat:enterprise\_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 42.91 seconds

//> The results of the nmap scan show that both port 80 (HTTP) and port 443 (HTTPS) are open.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

// Task 2

//> Number of Employees

- (11) fulltime employees

- upto (50) during seasonal

//> CEO

- (Minerva Camarena) is the sole owner of LV Clean Co

- She is a graduate of Francisco Gavidia University in San Salvador, El Salvador (1999-2005)

- She holds a BA in Educational Science with a major in English Language Teaching

- Her birthday is August 11th

//> CFO

- Sole Proprietorship (See CEO)

//> President

- Sole Proprietorship (See CEO)

//> Current Job Postings

- There are (NO current job postings)

- When available, jobs are posted through the main twitter account, locally on craigslist, and through indeed

//> Headquarters

- Headquarters at (150 East Liberty St Toronto, ON, Canada M6K3R5)

//> Sources

https://ca.linkedin.com/company/lv-clean-co-

<https://www.linkedin.com/in/minerva-camarena-43178326>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

// Task 3

//> Output the domain registration and hosting information

Domain Name: lvclean.ca

Registry Domain ID: 11601862-CIRA

Registrar WHOIS Server: whois.ca.fury.ca

Registrar URL: www.wildwestdomains.com

Registrar: Wild West Domains Canada, Inc.

Name Server: ns6005.hostgator.com

Name Server: ns6006.hostgator.com

DNSSEC: unsigned

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

// Task 4

//> Verify that the server can communicate with another computer or network

//> To confirm that the system can communicate we send a ping and append the output to this file.

PING 50.87.146.7 (50.87.146.7) 56(84) bytes of data.

64 bytes from 50.87.146.7: icmp\_seq=1 ttl=45 time=46.9 ms

64 bytes from 50.87.146.7: icmp\_seq=2 ttl=45 time=46.2 ms

64 bytes from 50.87.146.7: icmp\_seq=3 ttl=45 time=47.7 ms

64 bytes from 50.87.146.7: icmp\_seq=4 ttl=45 time=45.9 ms

64 bytes from 50.87.146.7: icmp\_seq=5 ttl=45 time=46.1 ms

64 bytes from 50.87.146.7: icmp\_seq=6 ttl=45 time=60.8 ms

64 bytes from 50.87.146.7: icmp\_seq=7 ttl=45 time=46.0 ms

--- 50.87.146.7 ping statistics ---

8 packets transmitted, 7 received, 12.5% packet loss, time 7010ms

rtt min/avg/max/mdev = 45.915/48.510/60.764/5.035 ms

//> The output shows us that the server is live and that it is able to communicate.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

//Task 5

//> Determine route from your local machine to the company’s network machine

//> To determine the route between our host and the target server, we use the 'traceroute' cmd

traceroute to 50.87.146.7 (50.87.146.7), 30 hops max, 60 byte packets

1 \* \* \*

2 10.78.5.93 (10.78.5.93) 1.381 ms 10.78.5.115 (10.78.5.115) 1.421 ms 10.78.5.125 (10.78.5.125) 9.714 ms

3 138.197.249.90 (138.197.249.90) 1.666 ms 138.197.249.86 (138.197.249.86) 12.324 ms 1.728 ms

4 toro-b1-link.ip.twelve99.net (62.115.9.209) 1.912 ms toro-b1-link.ip.twelve99.net (62.115.55.29) 1.895 ms toro-b1-link.ip.twelve99.net (62.115.9.209) 1.878 ms

5 level3-ic-361864-toro-b3.ip.twelve99-cust.net (213.248.94.123) 15.894 ms 15.880 ms 15.863 ms

6 ae2.3602.edge8.Denver1.level3.net (4.69.219.74) 59.598 ms 58.291 ms 58.248 ms

7 THE-ENDURAN.edge8.Denver1.Level3.net (4.53.7.174) 51.863 ms 51.800 ms 51.530 ms

8 69-195-64-111.unifiedlayer.com (69.195.64.111) 46.914 ms 69-195-64-113.unifiedlayer.com (69.195.64.113) 46.896 ms 45.940 ms

9 po99.prv-leaf1a.net.unifiedlayer.com (162.144.240.127) 47.074 ms po99.prv-leaf1b.net.unifiedlayer.com (162.144.240.135) 46.466 ms 46.402 ms

10 50-87-146-7.unifiedlayer.com (50.87.146.7) 56.206 ms 46.120 ms 46.116 ms

//> From the output we can see the route to the target machine

//> We note that there are around (30) hops preformed