Paul Polsinelli

IFT 302 43489

Sum 20

Lab 4

A.     TCP/IP Networking Utilities

Using Cybersecurity Essentials, by Brook, Grow, Graig, and Short, perform the Chapter 13 Hands On Exercise, found between pages 313 and 325.  When complete, answer the following questions.

1. Which command-line utility program is used to find the primary DNS suffix, IPv4 and IPv6 addresses for your computer?

Ipconfig. Typing “ipconfig /all” will give you all the network information. It can be used for identification, troubleshooting, and setup of a network.

The \_\_\_\_\_ ping\_\_\_\_\_\_\_\_ command causes a data packet to be sent to a specific IP address and then returns to the initiating machine.

Typing “ping” and the ip address of a device will send packets to the device and listen for a return. A successful round trip indicates functionality and connection of the device.

1. Which command detects whether routers along a communication path are functioning?

Tracert. Typing “tracert -h 10” and an URL will tell you how many hops to that URL and performance info on routers along the way.

1. Which utility program is used to examine current network connections?

Netstat. Typing “netstat” and an extention will tell you various information about data packets transmitted and received as well as connections.

1. The \_\_\_\_\_arp\_\_\_\_\_\_\_\_ utility is used to map IP addresses to MAC addresses?

Typing “arp -a” will display addressing information and map ip addresses to MAC addresses on the active network connections.

1. Which utility command is used to examine a list of all the shared devices on a LAN?

net view. Typing “net view” will list all computers on the LAN and their shared devices.

B.      Red Team Intelligence Gathering

Using the following tools, find and report the following for your favorite company:

|  |  |
| --- | --- |
| [**MxToolbox Supertool** (Links to an external site.)](https://mxtoolbox.com/SuperTool.aspx) | **MX Lookup**  **DNS Lookup**  **Reverse Lookup**  **DMARC Lookup**  **HTTPS Lookup** |
| [**Google** (Links to an external site.)](https://www.google.com/) | **Search:**[**What Is My IP? (Links to an external site.)**](http://lmgtfy.com/?q=what+is+my+ip&p=1) |

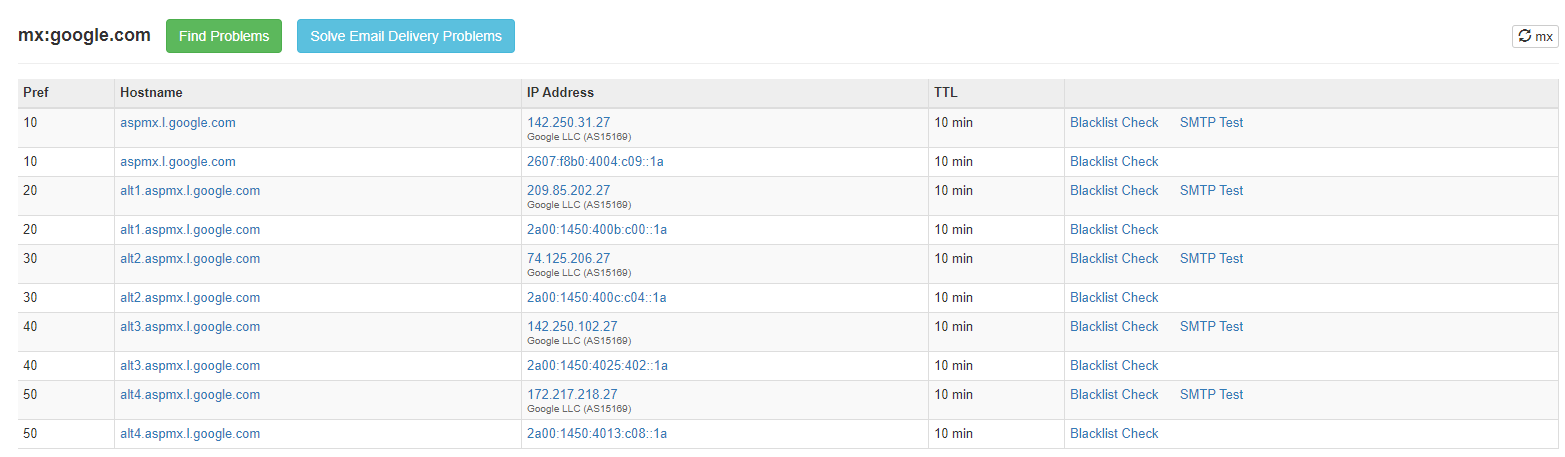
**Step 1:  Using the PING command from the above section, gather the IP address of Amazon.com, Microsoft.com, Google.com and/or your favorite web page.**

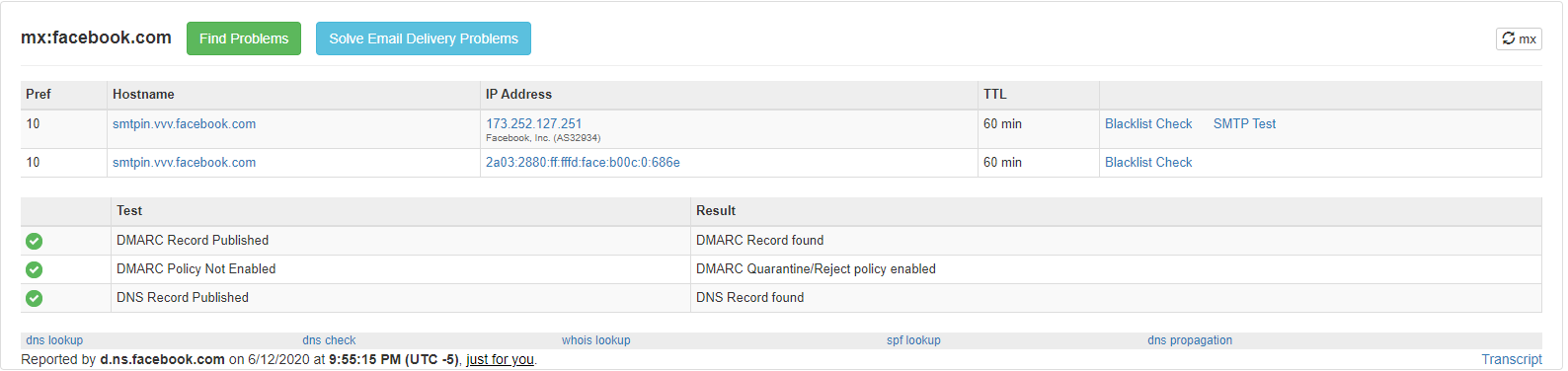
**Amazon.com – IP Address 176.32.103.205**

**Microsoft.com – timed out repeatedly**

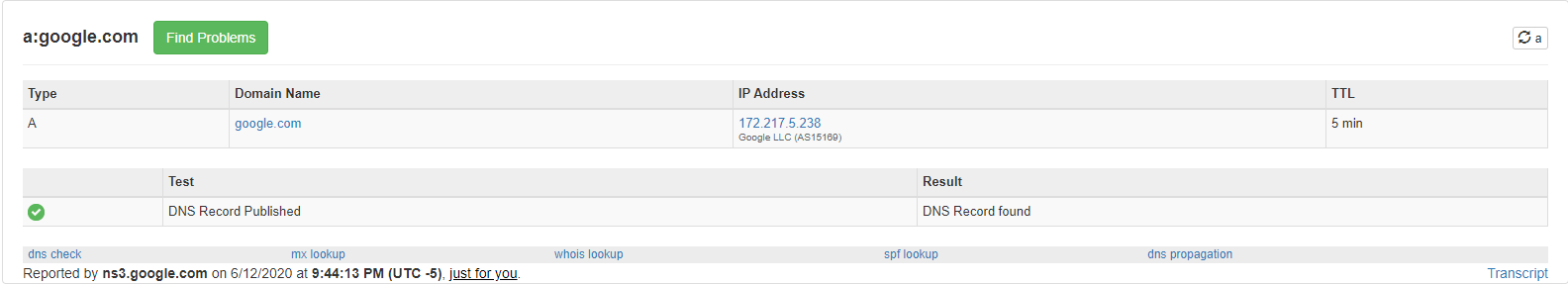
**Google.com – IP Address 172.217.5.238**

**Step 2:  Using the MX Toolbox.com Super Tool, lookup and provide the following for (A) one of the large companies mentioned above, as well as (B) one NOT mentioned above.:**

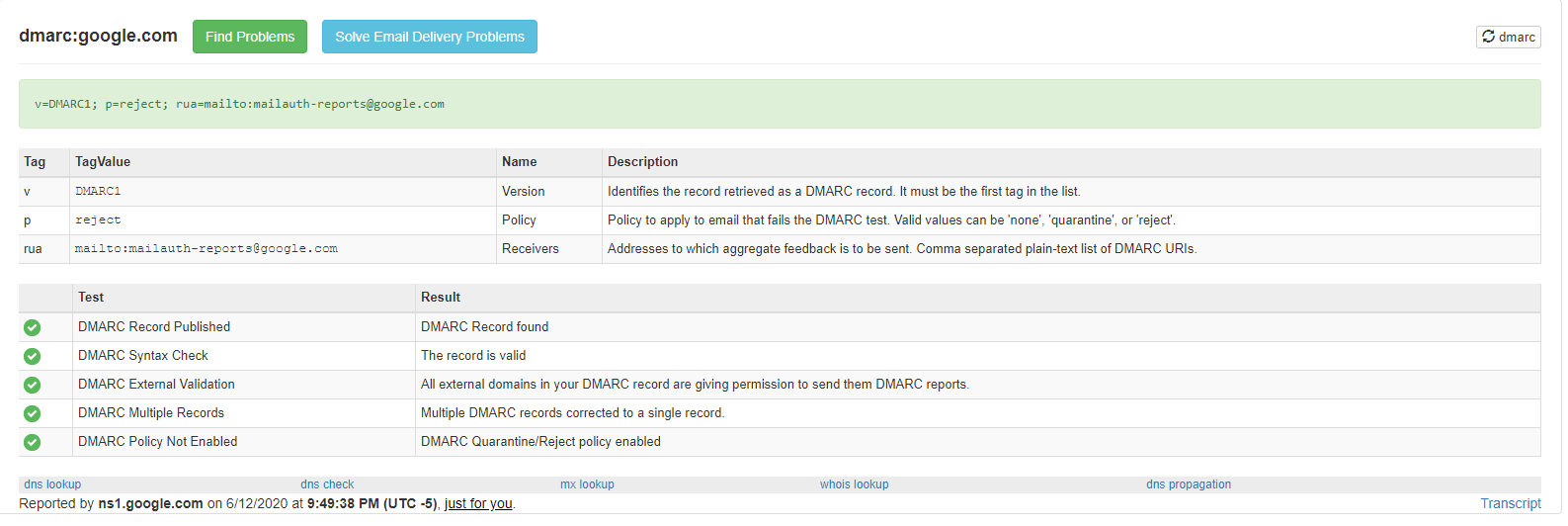
1. The MX servers used by the company 

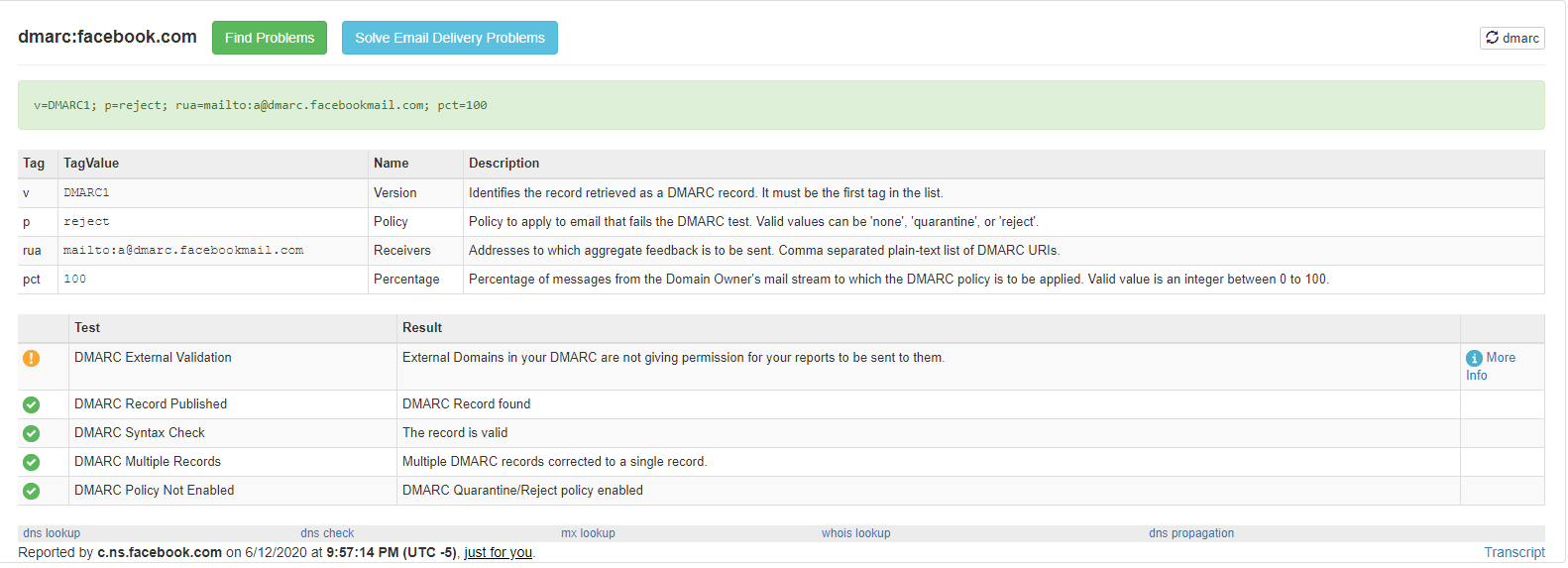


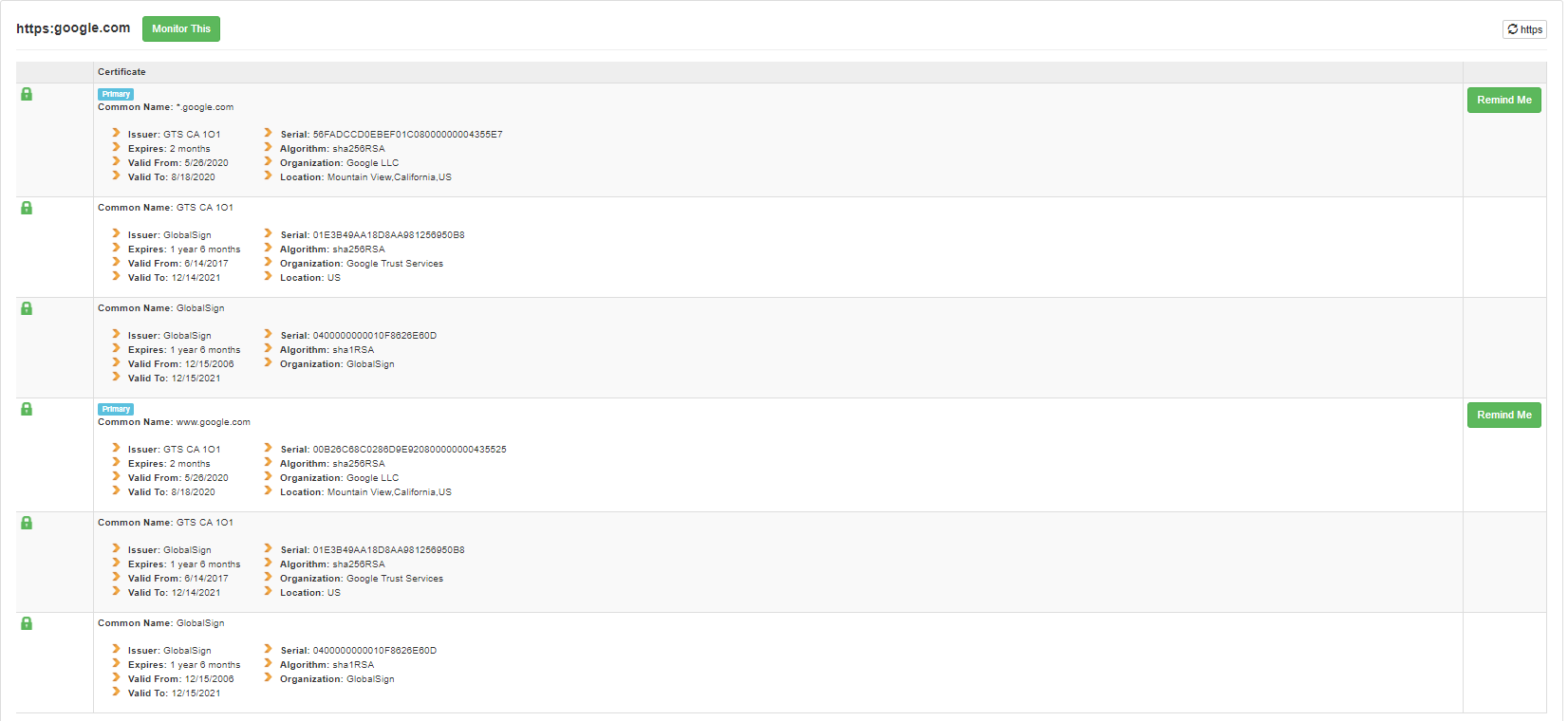
1. The DNS record

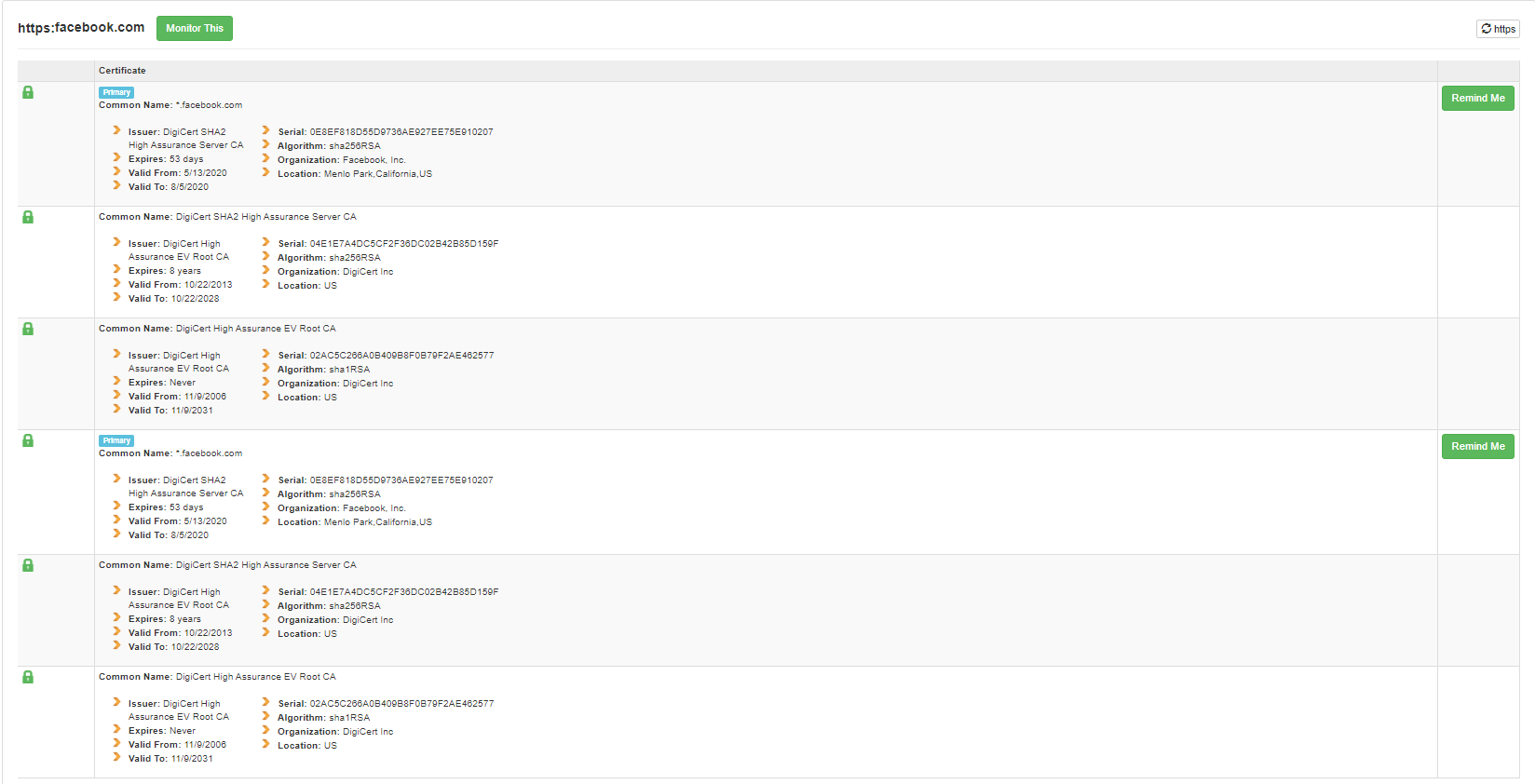




1. Whether DMARC technologies are being utilized 

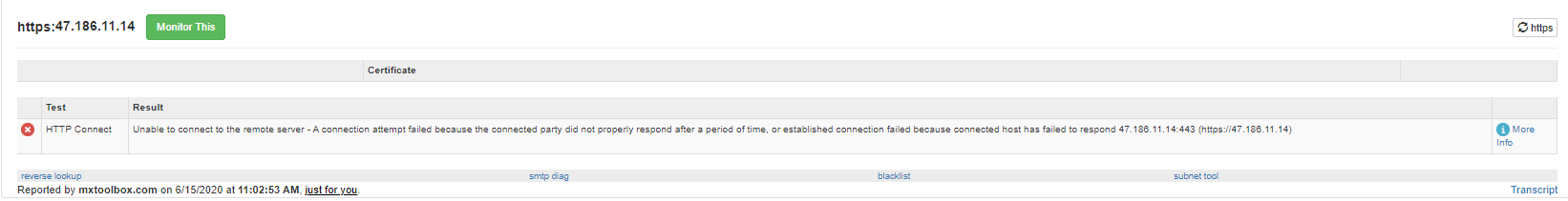


1. The status of the company’s TLS certificates (Hint: HTTPS Lookup) 



Also:

1. The reverse lookup report of your own web-facing IP address  
   (Hint: Use the above Google search). To comply with local national laws, students **not** in the US may wish to change their IP address before posting it in their deliverable.



**Example resources within the**[**MX Toolbox SuperTool (Links to an external site.)**](https://mxtoolbox.com/SuperTool.aspx)

C.      Terminology

Provide answers to the following questions.

* What is DMARC and why might it be needed?

Domain-Based Message Authentication Reporting and Conformance an email validation system that protects email domains from being spoofed, phished, and fall victim to other cybercrimes. (1)

* What is typosquatting?

Aka URL hijacking, is a form of cybersquatting. Basically is an URL that is really close to a popular website and disguised as it that waits for someone to mistype the real website’s URL and then performs a malicious activity on the hapless victim. (2)

* What is N+1 from an IT context and what is its value in ensuring availability?

N+1 is having the necessary structure required to provide service plus a redundancy in case of catastrophic failure of the primary system. (3)

* What security benefits does the cloud provide?

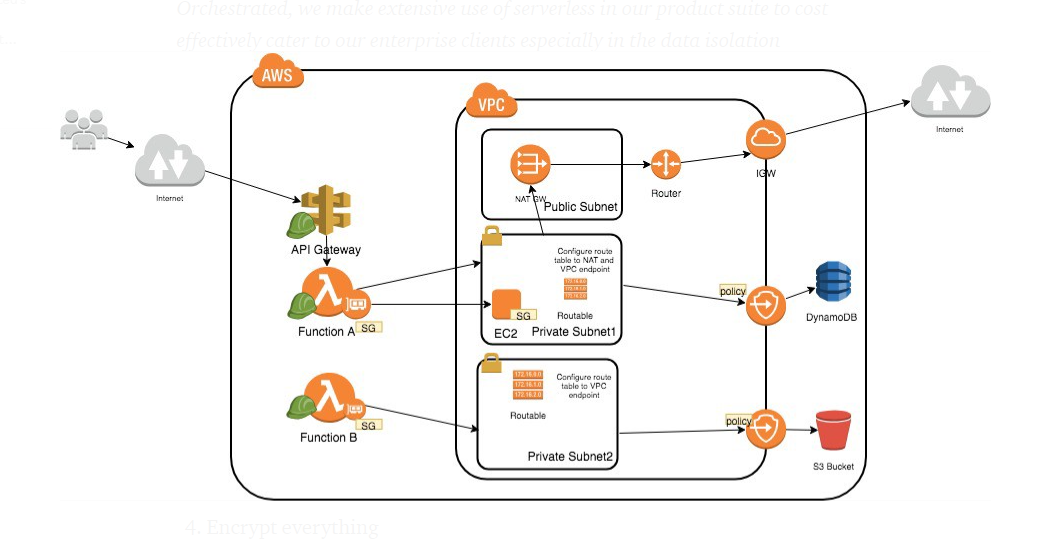
Cloud computing provides protection against DDoS attacks, data security, regulatory compliance, flexibility, and high availability and support. (4)

* What security disadvantages are inherent to the cloud?

Inherit disadvantages of cloud computing include loss of control, vendor lock-in, possible data loss, insider theft, data breaches, and unsecured Application Programming Interfaces (APIs). (5)

D.     Cloud infrastructure

Find a map of an AWS or Azure cloud infrastructure.  [Like this one (Links to an external site.)](https://raw.githubusercontent.com/open-guides/og-aws/master/figures/aws-data-transfer-costs.png).  [Or this one (Links to an external site.)](https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/aws-reference-architecture-patient-engagement.pdf).  [Or this one (Links to an external site.)](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/media/workday-inbound-tutorial/wd_overview.png).  Explain how or where this infrastructure might be insecure or more secure compared to a similar on-premises solution.  What could be done to improve the security of design, if not already listed on the diagram?



To increase security on this network include the following steps

1. Apply principle of least privilege to functions A and B as they provide access to the interior functionality of the AWS system.
2. Minimize the functions exposed through the API gateway to reduce attack surface.
3. Route traffic within AWS as much as possible instead of over the internet to prevent data exposure.

(6)

E.      Emphasis on HTTPS

Using the nakedsecurity link in the resources section describe why you believe that Google decided to reduce its page ranks for sites that are not HTTPS-enabled.

I believe Google’s decision to reduce page ranks for non-HTTPS sites is to standardize TLS protocol and get rid of HTTP. HTTP is sort of the wild west of internet protocol. It transmits in plain text. The more secure businesses are on the web, the more ecommerce will increase, and the more Google’s necessity will increase. Perhaps most importantly to Google is the fact that as the industry grows because of the security, it’s ad revenue will increase as more ecommerce companies are created and expand and need to advertise and direct traffic to their sites. HTTPS is the tide that floats all internet boats.

References

1. What is DMARC?, mimecast, <https://www.dmarcanalyzer.com/dmarc/#:~:text=DMARC%20(Domain%2Dbased%20Message%20Authentication,phishing%20scams%20and%20other%20cybercrimes.&text=DMARC%20adds%20an%20important%20function%2C%20reporting.>, 2020
2. What is Typosquatting?, McAfee, <https://www.mcafee.com/blogs/consumer/what-is-typosquatting/>, Jul 3, 2013
3. Mike Allen, Redundancy: N+1, N+2 vs. 2N vs. 2N+1, Datacenters.com, <https://www.datacenters.com/news/redundancy-n-1-n-2-vs-2n-vs-2n-1-part-ii#:~:text=N%2B1%20represents%20the%20amount,flat%20with%20a%20spare%20tire.>, 2020
4. Steve Walker, 5 Benefits of a Cloud Computing Security Solution, TBConsulting, <https://blog.tbconsulting.com/5-benefits-of-a-cloud-computing-security-solution#:~:text=A%20cloud%20computing%20solution%20provides,back%20down%20to%20reduce%20costs.>, May 20, 2019
5. Natalie Boyd, Six Security Disadvantages of Cloud Computing, sdxcentral, <https://www.sdxcentral.com/cloud/definitions/security-disadvantages-cloud-computing/#:~:text=Loss%20of%20Control%3A%20The%20enterprise's,(CSP)%20and%20the%20enterprise.>, Aug 2, 2018
6. Pim Amponpun, Steps to Secure AWS Serverless- Lambda (Part 1), orchestrated, <https://medium.com/orchestrated/steps-to-secure-aws-serverless-lambda-part-1-a6e5d1b05f45>, Oct 16, 2018