Sarah Tse
ITSS 4V95

Assignment 4: Networking Basics

Total Points: 20

1) **Why is understanding computer networks critical to IT security? (5 points). (1 – 2 pages long)**

   Networks are what connect us to one another. However with these connections there are new ways for unauthorized users to gain information and access that could potentially harm others. Understanding computer networks is critical to IT security because it helps IT Security professionals perform vulnerability and risk assessments, know how to prevent and mitigate attacks and educate those outside of security on what to do.

   One of the first tasks a company will do to build a security program is to perform a vulnerability and risk assessment to determine what they need to protect and how to do this by putting controls in place. Part of this assessment is identifying the assets that have vulnerabilities that could be exploited and knowing what impact it has on the company. Having a good foundation in computer networking helps professionals know of the assets, how they are connected and rank them on importance. For example, a server may have a higher risk than a company issued laptop because the server is connected to other servers in a farm or have a higher level of access.

   Secondly, understanding networks helps in knowing how attacks happen as well as how to mitigate and prevent them. When we hear about cyber attacks, immediately there is a shroud of mystery that covers how the attack was conducted when in reality, the key to it all is the network. Networks are what make companies weak because if there is one vulnerability on one machine, then it can be exploited to gain access or information to other machines on the network. For example, one of the biggest attacks this year was Capital One's incident which was caused by a malicious insider exploiting a misconfigured web application firewall(Brandom, 2019). Even though networks are a problem in security, it is a solution to better productivity and connectivity in the workplace. Therefore, it is worth spending time to understand networks, so organizations can better understand how to secure the network from attacks and breaches.

   Lastly, as networks are one of the foundations to IT security, knowing how they work will better prepare security professionals to educate a variety of users. In a recent survey of DEFCON attendees, 84% of the respondents said they use social engineering as part of their attack strategy(Goldman, 2017). While an organization can have the most secure network and systems, humans are still a big risk to the organization, especially if they are uneducated. By spending the time to educate users, organizations can effectively lower that risk and better control it. Hence, knowing about networks can help professionals simplify the explanation on how attacks happen for the non-technical users.

   In conclusion, understanding networks is important for IT security because it helps perform accurate vulnerability and risk assessments, evaluate how attacks happen and how to prevent them and better prepare professionals to educate non-technical users.

Sarah Tse
ITSS 4V95

2) Describe the OSI model and the functions handled within each layer. Explain the concept of "encapsulation/ de-capsulation" in the OSI model. (15 points) (2 -4 pages long).

The Open Systems Interconnection(OSI) model was created by the International Organization for Standardization (ISO) to establish a common communication standard apart from the government and for protocol developers. The model features seven different layers that each have a separate function to facilitate data transfer.

The first of the seven layers is the application layer which is responsible for providing tools or services for the user. Within the model, there isn't an official start or end layer but in terms of sending data, this would be the first layer. To explain the full functionality of the OSI stack, refer to requesting a webpage such as Google. When a user types in "google.com" in the search bar, the web browser will use the Domain Name System protocol to find the site and the information the user is looking for. Using Wireshark, I was able to capture the data packets leaving and entering my laptop when requesting google.com. As seen below, there is a response that gives my laptop the address for "google.com" at 172.217.14.174.

Time	Source	Destination	Protocol	Length	Info
2.493478	192.168.1.5	192.168.1.1	DNS	70	Standard query 0xf550 A google.com
2.524512	192.168.1.5	192.168.1.1	DNS	70	Standard query 0xf550 A google.com
2.557113	192.168.1.1	192.168.1.5	DNS	86	Standard query response 0xf550 A google.com A 172.217.14.174

Figure 1

Next is the presentation layer which is responsible for taking data from the application layer and encoding and compression of data files and ensuring that both systems support the file formats requested. Continuing with the same example from above, this layer would be responsible for encoding the data so that the destination (domain name system server) can understand the request. If I were on the receiving side, this layer would reconstruct the google logo using an image file located within the data stream.

The data is then passed onto the session layer which is responsible for starting, maintaining and stopping communications between the sender and receiver. If some of the data stream isn't transmitted, the session layer will initiate for another delivery. Data is sent in a stream using either half duplex, full duplex or simple communication. For a request to "google.com", this layer would be responsible for opening sessions with different servers to send data to.

Once a session is established, the transport layer is responsible for taking the data stream and breaking it down into numbered segments using session rules. These session rules specify how much data to put in each segment, how to verify the data sent and if a segment is lost. After the data stream is segmented and numbered, the proper source and destination ports are added in the header. The difference between the session and transport layer is that the transport layer is only responsible for one pair of source and destination ports. The session layer coordinates all of the required sources and destinations(Elbert, 2018). In the figure below, the red boxes highlight the TCP segments that were received and sent. Within the "info" column, there are SYN, SYN-ACK and ACK

messages that represent the three way handshake between my laptop and “google.com”.

Time	Source	Destination	Protocol	Length	Info
4.199254	192.168.1.5	184.72.104.138	TLSv1.2	128	Application Data
4.208507	192.168.1.5	172.217.14.174	TCP	66	33303 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4.208837	192.168.1.5	172.217.14.174	TCP	66	33304 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4.213188	192.168.1.5	172.217.6.164	UDP	1392	64051 → 443 Len=1350
4.216245	192.168.1.5	172.217.6.163	UDP	1392	64052 → 443 Len=1350
4.219251	192.168.1.5	192.168.1.1	DNS	85	Standard query 0xd2ff A lh3.googleusercontent.com
4.221137	192.168.1.5	192.168.1.1	DNS	75	Standard query 0x85dc A apis.google.com
4.226237	192.168.1.5	192.168.1.1	DNS	86	Standard query 0xce58 A encrypted-tbn0.gstatic.com
4.231561	172.217.14.174	192.168.1.5	TCP	66	80 → 33303 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=…
4.232055	192.168.1.5	172.217.14.174	TCP	54	33303 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4.237885	172.217.14.174	192.168.1.5	TCP	66	80 → 33304 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=…
4.238075	192.168.1.5	172.217.14.174	TCP	54	33304 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4.238214	216.58.194.46	192.168.1.5	UDP	62	443 → 52228 Len=20

Figure 2

Below the Transport Layer is the Network Layer which is responsible for “routing and addressing information.” A segment from the transport layer will turn into a packet once the source and destination addresses (usually IPv4 or IPv6) are added. The hardware used at this level are routers and can determine the best possible path between two devices. Continuing with the example, within the TCP packet, the IPv4 header is viewable which shows the source and destination IP addresses. In this case, this information is used to get the packet from my computer to the server.

```
    90 4.237885   172.217.14.174  192.168.1.5     TCP        66 80 → 33304 [SYN, ACK] Seq=0 Ack=1 Wir
    91 4.238075   192.168.1.5     172.217.14.174  TCP        54 33304 → 80 [ACK] Seq=1 Ack=1 Win=1310
    92 4.238214   216.58.194.46   192.168.1.5     UDP        62 443 → 52228 Len=20
    93 4.239197   192.168.1.1     192.168.1.5     DNS       112 Standard query response 0x85dc A apis
> Frame 90: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Netgear_71:7b:1f (3c:37:86:71:7b:1f), Dst: IntelCor_e8:c3:30 (88:78:73:e8:c3:30)
v Internet Protocol Version 4, Src: 172.217.14.174, Dst: 192.168.1.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xe685 (59013)
  > Flags: 0x0000
    Time to live: 118
    Protocol: TCP (6)
    Header checksum: 0xe109 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.217.14.174
    Destination: 192.168.1.5
```

Figure 3

Next, is the Data Link layer that is responsible structuring the packet into the proper format to be transmitted at the physical layer. The formats are based off of the hardware and is required so that at the destination hardware can understand what is being requested.

```
> Frame 90: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
v Ethernet II, Src: Netgear_71:7b:1f (3c:37:86:71:7b:1f), Dst: IntelCor_e8:c3:30 (88:78:73:e8:c3:30)
  v Destination: IntelCor_e8:c3:30 (88:78:73:e8:c3:30)
      Address: IntelCor_e8:c3:30 (88:78:73:e8:c3:30)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Netgear_71:7b:1f (3c:37:86:71:7b:1f)
      Address: Netgear_71:7b:1f (3c:37:86:71:7b:1f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.217.14.174, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 33304, Seq: 0, Ack: 1, Len: 0
```

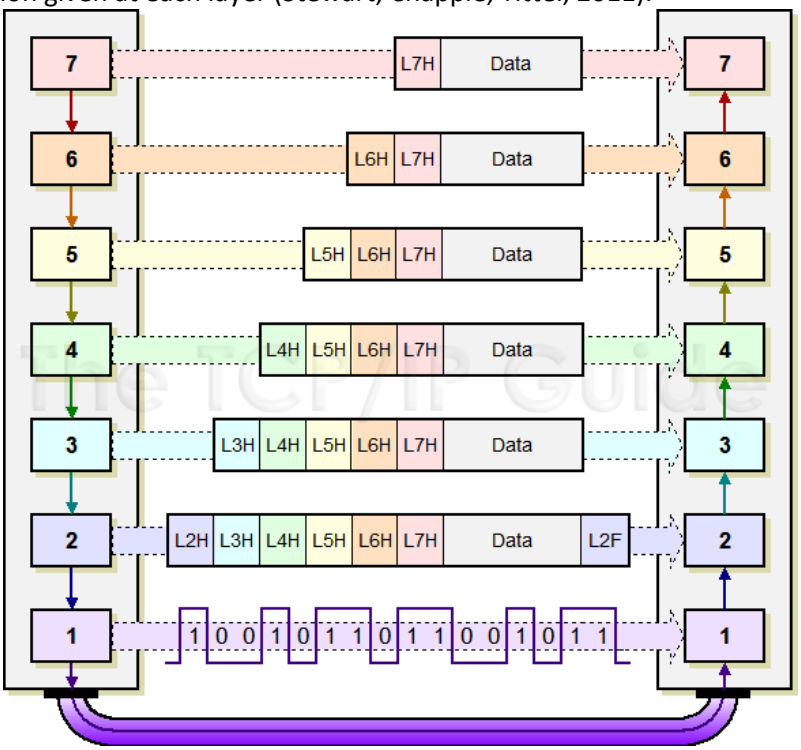
Figure 4

Looking at the same TCP segment within Wireshark, we can drill down into the Ethernet frame and view the destination is my computer’s network card media access control (MAC)

address. The source of the packet came from one of Google's server that uses a Netgear device.

The last layer in the stack is the physical layer which is responsible for translating the frame, from the previous layer, into bits. This layer is named "physical" because the bits travel a physical medium such as coaxial cables or fiber optics. The devices on the ends of these cables also control throughput and noise and determine when to use analog or digital signals.

Each layer of the OSI model that the data package goes through will get more and more information added to it known as the "header". This idea is called encapsulation and its counterpart is decapsulation where the headers are stripped at every layer. In the request for "google.com" example described above, each layer adds a little more information so that when it is sent as bits at the physical layer, the receiving device will know what to do with the information given at each layer (Stewart, Chapple, Tittel, 2011).



Sarah Tse
ITSS 4V95

References:

Brandom. Russell. (2019, Jul. 31). The Capital One Breach is more complicated than it looks. Retrieved from https://www.theverge.com/2019/7/31/20748886/capital-one-breach-hack-thompson-security-data

Dordal, Peter L. (2019, Jul. 26). An Introduction to Computer Networks (Release 1.9.19). Retrieved from http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf

Elbert, Sybille. (2018, Mar. 18). What is the difference between session layer and transport layer in the OSI model?. Retrieved from https://www.quora.com/What-is-the-difference-between-session-layer-and-transport-layer-in-the-OSI-model

Goldman, Jeff. (2017, Feb. 28). Fully 84 Percent of hackers leverage social engineering in attacks. Retrieved from https://www.esecurityplanet.com/hackers/fully-84-percent-of-hackers-leverage-social-engineering-in-attacks.html

Kb, Sunil. (2014, Oct. 3). What is the role of OSI layers when we open a webpage?. Retrieved from https://www.quora.com/What-is-the-role-of-OSI-layers-when-we-open-a-webpage

Reference. (n.d.). What Is the Function of Session Layer? Retrieved from https://www.reference.com/technology/function-session-layer-4f33690ec959af3c

Stewart, J., Chapple, M., & Tittel, E. (2011). *CISSP : Certified Information Systems Security Professional : study guide* (5th ed.). Indianapolis, Ind: Wiley Pub.