METHODS OF NETWORK ANALYSIS

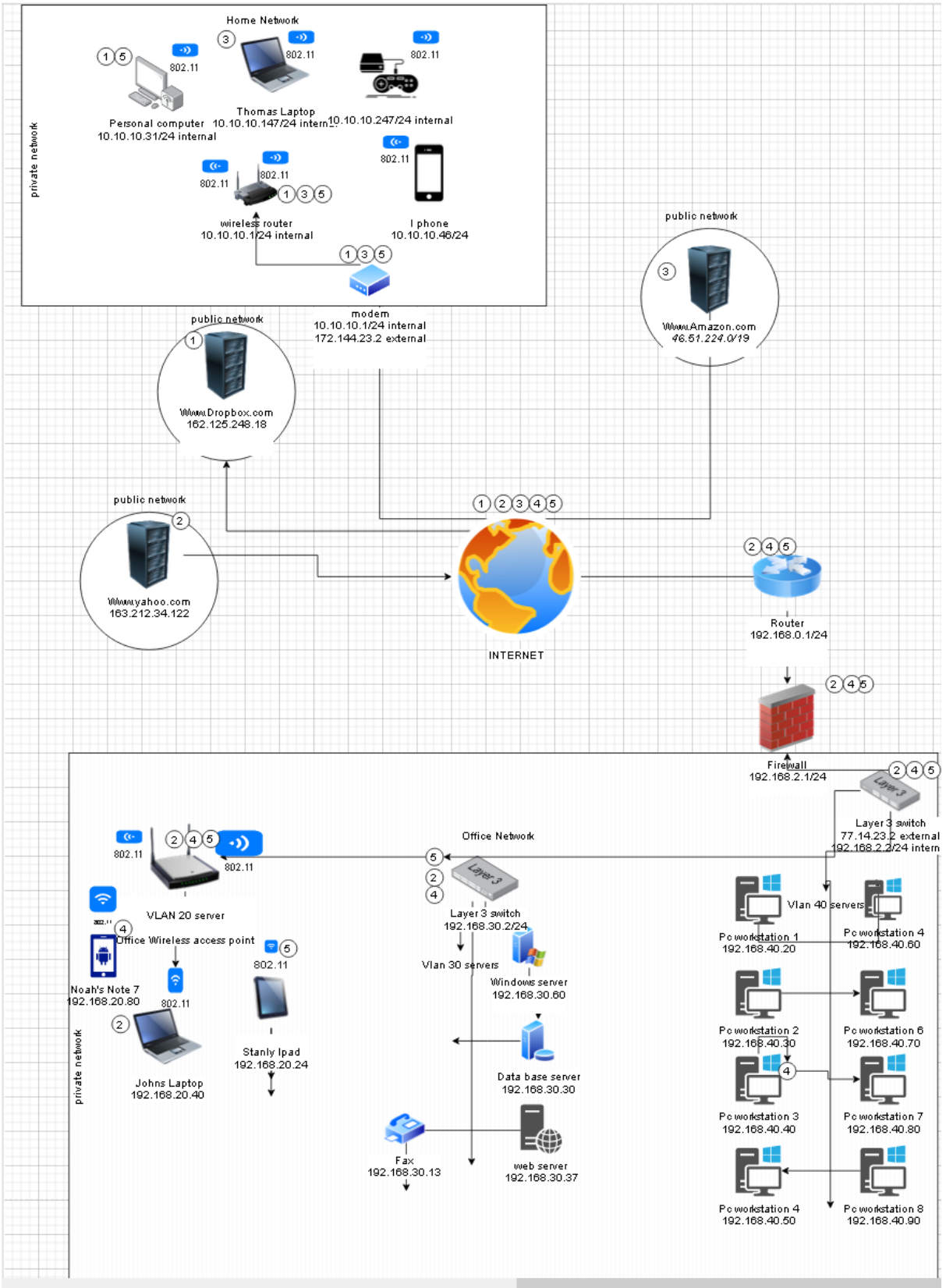
Christopher Wilson

University of Arizona

CYBV #326 INTRODUCTORY NETWORK ANALYSIS

Michael Galde

May 7, 2023


Home Network
802.11
Personal computer
10.10.10.31/24 internal
Thomas Laptop
10.10.10.147/24 intern
802.11
10.10.10.247/24 internal
802.11
802.11
802.11
wireless router
10.10.10.1/24 internal
I phone
10.10.10.46/24
private network
modem
10.10.10.1/24 internal
172.144.23.2 external
public network
www.Dropbox.com
162.125.248.18
public network
www.Amazon.com
46.51.224.0/19
public network
www.yahoo.com
163.212.34.122
INTERNET
Router
192.168.0.1/24
Firewall
192.168.2.1/24
Layer 3 switch
77.14.23.2 external
192.168.2.2/24 intern
Office Network
Layer 3 switch
192.168.30.2/24
Vlan 30 servers
Windows server
192.168.30.60
Data base server
192.168.30.30
web server
192.168.30.37
Fax
192.168.30.13
Vlan 40 servers
Pc workstation 1
192.168.40.20
Pc workstation 4
192.168.40.60
Pc workstation 2
192.168.40.30
Pc workstation 6
192.168.40.70
Pc workstation 3
192.168.40.40
Pc workstation 7
192.168.40.80
Pc workstation 4
192.168.40.50
Pc workstation 8
192.168.40.90
802.11
802.11
VLAN 20 server
Office Wireless access point
802.11
Noah's Note 7
192.168.20.80
802.11
Johns Laptop
192.168.20.40
802.11
Stanly Ipad
192.168.20.24
private network

Concepts

1. Monica would like to open to submit a file to www.Dropbox.com at the application layer as the client; we request to transfer our file to the server. She uses her home computer, but Monica's IP address is private and must be public for her work to get to Dropbox. Once at the transportation layer, the file will be broken down into packets, and with the help of the TCP protocol, we will have reliable transportation to the client-server along with the 3-way handshake. Still, it would help if you used NAT (network address translation) for that to happen. A private IP cannot just go to Dropbox whenever it wants to access the internet. It must send a request to the router, which takes its public IP address and forwards it to the Dropbox website. Typical web dropboxes only use two ports for communication ports: port 80 and port 443 with the link layer where we would get the most security along with implementing other measurements. For you to make a stable and reliable connection to the server, it will then use the Transport control protocol, ensuring that it gets to the Dropbox website with no errors. Also, TCP includes error checks mechanisms to ensure that the data you send has made it without errors at the link.

2. John would like to access www.Yahoo.com so that he can access his Yahoo mail, but John needs to make sure he can get out onto the web. To get there, he must request the router change his so that his ip goes from the router instead of the computer IP from a private into a public IP address. That is where the application layer comes into play to know what happens

there. First, it has to go through the firewall. Once out, it will then have to use IMAP protocol for it to be able to receive the message that it has opened for the others to see. For Imap, the port that is used for incoming mail would be using port number 993, and in cases where you would need to make sure that the message is secure and can go through, the port number will change to port 995, depending if your plan on using a single device to look at the document or if you plan only having that document on one computer such as johns company computer that he keeps at work. You wanted to keep those emails safe from outsiders.

Once there, the link layer, that is, when it is on the local network, we can transfer data using wifi or ethernet.

3. Thomas wants to buy a new keyboard on www.Amazon.com, so Thomas uses his laptop in his house and decides to place the order on his laptop; the first thing that will happen is that the application layer uses the HTTP protocol, and he will receive an email confirming that the keyboard he just bought has been confirmed by sending him an email. However, at the same time, you send the order you just placed to Amazon using a secure protocol known to Amazon called APIs. After receiving the handshake, we now use the internet layer to ensure that we can send our data, which will allow you to utilize amazons own ordering system that takes orders, and checks the inventory to make sure that the

quantities of the products are always up to date .but for use to make a communication with the amazon servers we will have to get out to the internet which will have to turn our private IP on to a single public IP using an ipv4 ip addressing to contact the servers using the HTTPS port 443 on the server side once that is done we now can look at the information on our local machines.

4. Noah has recently moved and has to update his personal information, so he is sending his information over to the hr department to fix the required info, but we do not have to leave our network. Except to connect with the email server on the side of the server. In this case, the application layer is responsible for initiating and controlling the email and email transfer processing by going out to the server for that client. It uses protocols like the STMP and sends it over the private network. Using the transportation layer Tcp to establish reliable transportation within the internet layer, we can expect that routing data is responsible for transporting the email within the same network at the link layer. We can use the wifi on the network to send it to the workstation.

5. Thomas has sent his friend Stanly a link to his iPad, which is on a private network from his computer at home; Thomas needs to learn that the website he sent to Stanley was infected with malware that can spread quickly onto the company's servers. At the application layer, we can send over an that could include an infected website. Still, Thomas had no clue that it was infected by some spyware that can not only be hard to detect without certain technologies but can collect much data and personal information. For transportation, it stays the same while using the Transportation control protocol. With the internet layer, it has then broken down and sent in packets over the internet. Once that is done, it is up to which protocol it wants to use. In the case of using the internet services that send the email, it would be port 443. once it gets inside the system, it can use any vulnerabilities that it can find, such as software that has not been updated for a while, until it is detected within the system. Furthermore, when it hits the link layer of that network, then it will be able to move around to other machines on the same network to make other workstations get infected.

Research and Analysis

When we discuss the different types of attacks that we can encounter and affect the TCP/IP model, we can discuss the four following layers of the model. The

application layer, The transportation layer, the Internet layer, and the network interface. Each of these different layers can be attacked on each layer.

The Application layer

It can be found in the last layer of the OSI model. It is not the most secure layer due to back-and-forth communication using UDP. (DuBois,2006) Attacks can happen at the application layers and are hard to detect due to a lack of detection software and hardware. The most common attack is called a SQL attack. The way that SQL attack happens when an attacker wants to inject a Malicious type of SQL code inside of a web applications input field to try to trick the system into executing an unintended SQL command; then, whenever the attacker gets into the system, they will get the chance to modify anything they see fit. The reason that this happens is due to the coding that is put into use. (Stevens, fall,2006) With this attack, the attacker hopes to disrupt confidentiality and integrity, depending on the overall goal of the attack. In the case of network vulnerability, it takes advantage of the leak of PI and sensitivity data exposure. In this case, what we can do to mitigate the attack on this layer is we can implement a firewall that has more robust security parameters in place to block any unwanted traffic that is starting to come in from outside sources. (Liska Gates,2018)

The Transportation layer

Inside the fourth layer lies the transportation layer, which provides transparent data transfer to all end users. In layer four, the most common attack on this layer is a Distributed denial of service (DDoS) attack. In this attack, there is no real target. Instead, the attackers are trying to compromise the A part of the CIA triad by overwhelming the system with a flood of traffic from multiple sources, making it difficult for legitimate traffic to reach the server; these attacks are called SYN floods(Edwards,2009). With this, it will eventually stop responding to legitimate requests and effectively deny access to that service. A DDoS attack can happen at any level of the OSI model but tends to happen more frequently on the transportation layer(Bramante,2009). In the transportation layer, when targeted, it typically tends to go after the UDP or TCP protocols. With a DDoS attack, there are a few ways that we can prevent these from happing. First, lower the number of open ports; that way, we lower the network's attack surface and lower the chance that an attack can happen. Also, include some new rules implemented inside the firewall; you can easily add traffic filtrations into the system. (Bramante,2009) You will likely reduce the amount of legitimate traffic to focus on the concerning traffic.

The Internet layer

The TCP/IP model Internet layer is in the three-layer that form the OSI model; in this layer, it is responsible for carrying data packets across the network in the internet, the logical addressing scheme that enables the data packet that allows it to be routed across multiply networks to reach the destination of the network. (Donahue,2011) One method for attacking the third layer of the OSI model is IP Spoofing. We can deceive the target network into accepting the packets as legitimate packets with IP Spoofing. With this IP source, it is

supposed to look like a trusted IP address; along with having to worry about IP spoofing, we also have to worry about attackers using a combined attack such as phishing to ensure that the attacker can only limit the amount of damage that they can do to a single entity or organization. (Stevens, fall 2011) When we ask ourselves what the plans are with IP spoofing, we know that it is going into a network that wants to keep secrets in the network, so getting into it would be a breach of confidentiality of the CIA triad. However, a few vulnerabilities come up in taking advantage of our network; IP spoofing can evade any network detection and bypass specific security controls such as firewalls and access controls. (Bramante, Edwards,2011)

We can combat IP spoofing by using certain types of filtering, such as ingress filtering, that will allow us to drop any packet that seems to be a spoofed source address, and this filtering can be implemented at the ISP level, or it can be implemented into the network itself.

Network interface

The TCP/IP first layer of the OSI model is called the network interface layer; this layer is responsible for multiple things on this layer. For example, it can handle error detection and data correction. The attacks on this layer are widespread and tend to happen very frequently on this layer. One of the attacks is called a Man-in-the-middle attack. A MitM attack is an attacker communication interception between two different places, such as clients and servers, and they can modify, inject information, and eavesdrop on a conversation. (

Stevens,2006) In this attack, we also know that in a MitM attack, the attacker can steal information such as login information or be redirected to websites with malicious malware. With the Cia triad, we can tell that it compromises confidentiality because other people can read the conversation. On the other hand, the network advantage is that it can be in a private or public network and is hard to detect by using HTTPS. (Liska, Gates,2018)

A couple of things we can implement to help mitigate the attack. First, we need to implement encryption with all of our data; next, we need to use digital certificates to ensure we receive what we receive from the correct user. Lastly, we can implement a Two-factor authentication to add another security to lower their chances of success.

References

Clarke, J. (2009). Blind SQL Injection Exploitation Chapter 5. In *SQL injection attacks and defense 2nd edition*. Essay, Elsevier Science.

Donahue, G. A. (2011). *Network warrior*. O'Reilly.

DuBois, P. (2006). *MySQL cookbook*. O'Reilly.

Edwards, J., & Bramante, R. (2009). Chapters 8,9,10,11. In *Networking self-teaching guide: OSI, TCP/IP, LANs, Mans, wans, implementation, management, and maintenance* (pp. 454–614). essay, Wiley Pub.

Fall, K. R., & Stevens, W. R. (2011, November). *TCP/IP illustrated, volume 1: The Protocols, 2nd edition*. O'Reilly Online Learning. Retrieved May 7, 2023, from https://learning.oreilly.com/library/view/tcp-ip-illustrated-volume/9780132808200/ch05.xhtml

Gates, S., & Liska, A. (2018, July). *Securing web applications*. O'Reilly Online Learning. Retrieved May 7, 2023, from https://learning.oreilly.com/library/view/securing-web-applications/9781492040279/