OREGON STATE UNIVERSITY

CS 373

WINTER 2019

Week 6

Author:
Thomas Noelcke

Instructor:
D. Kevin McGrath

I. Overview

This week we are doing an overview of network security. To really dive deep into network security would probably take a course if not several courses or maybe even a PHD. This week I will discuss parts of the lecture that I found interesting along with listing out new terms that I learned through out the lecture. I will not discuss the lab this week as we are turning in the lab as its own assignment.

II. Interesting Lecture sections

III. Why bother with network security?

We just spent a bunch of time looking at detecting malware on hosts. So why would be bother with network security? We may want to prevent that malware from getting there in the first place. We may also want to secure data going in and out of our network. We also want to prevent denial of service attacks. Along with many other reasons.

IV. Robustness Principle

This comes from the origin of the internet. How can we build a system that every one can use where different pieces of software can communicate. The idea is to be Liberal in what we accept from the outside and conservative in what we send out on to the network. This principle has formed much of the internet that we know and love today. This has made it easier to communicate with other systems but has also made it easier to preform network based attacks. In this section we also talked about the fact that this principle has driven the idea of backwards compatibility. This has lead to many different vulnerabilities.

V. Protection Strategies

A. Positive Mode Policy

This is another term for white listing. This is where we have a policy where only things that are on the white list are allowed to run. This allows the network to filter out only the data that is allowed to access the network through the network. This is done by they firewall. Using this strategy the defender has the advantage because the creator of the network knows what the network is for. The attacker doesn't know what my network is for. So the second that you use my server in a way that I didn't intend I can shut it down. We also discussed the idea of an attack surface. This idea is that there is a certain amount of my network that you can see and I can limit how much of this is exposed to the outside world based on what my network is for. Part of the reason this approach is good is that the way that a network can be attacked is infinite, the way a particular network can be used correctly is finite.

B. Firewalls and Security Zones

It is common to define zones in the network where different policies apply. Firewalls are devices that sit between the zones and filter traffic based on the network policy. Below is a list of commonly used zones:

- Internet
- Intranet
- Testing Labs
- Extranet
- Corporate
- Data Center
- DMZ
- User Stations (DHCP Pools)

Once you have created these zones the firewall can create rules on what actions can be taken in each zone. This is mostly done based on what protocols are used. Such as my mail server shouldn't have an ftp type connection made to it so I wouldn't allow this type of traffic in my mail server zone.

C. other firewall like devices

There are devices that are like firewalls but aren't really firewalls. Below is a list of such devices:

- Proxies (Web Gateway) - This allows us to monitor web traffic an look for different technologies that might be causing problems.
- Email Gateway - This is similar to a Proxy however this is for mail rather than general internet traffic. This allows us to filter all the mail and determine what is valid mail and what isn't valid.

D. defense in depth

This is an old principle that was described with an old picture of a castle. This idea is that you have layers of defense. For instance its like gondor which has rings of security. Defense in depth allows us to protect our network using different rings of security. This means that an attack takes more than one layer of security to get through to be successful. This concept is really important. When designing a network that is the right time to design the security. Its also important to note that this must also be done iterativily. Even if you design the best security you will still get penetrated. You need to as you get penetrated examine what happened and what I can do to prevent that from happening again in the future.

E. Intrusion Detection and Prevention System

Intrusion detection systems generally block traffic by finding things that we know are bad and blocking them. This differs form a firewall because firewalls generally only look at what we want to explicitly allow on a network. So in general we can say that IPDS's tend to black list where firewalls white list. Its also important to note that this system also collects information on what attacks and what is being attacked. This works great for threats that are well defined and have been detected before. This doesn't work well for Zero Day Attacks. Another problem with IDPS is false positives. This is where traffic you intended and is legitimate is blocked as a threat.

F. Honeynets / intrusion detection

In this strategy we put a fake machine that looks like something that someone might want to attack. We can put fake data on this and make it look more interesting but really just wastes the attackers time. This is essentially a trap where we put out some bait out and then trap the attacker on the Honeynets. This has some problems as it can cause some one who is doing things that are legitimate but get caught in the honey net instead of getting where they wanted to go.

G. Quarantine

If I put something in quarantine I am essentially putting a host who is behaving badly in time out and monitoring what they are doing. This prevents them for infecting any one else on my network or doing any sort of other damage. This form of protection is commonly applied on network entry. Some times firewalls will institute a blacklisting mechanism that is similar to quarantine.

H. Reputation

In this scheme we use big data to solve the security problem. We create a list of good things and bad things. This list is then served from the cloud. We then use this information to associate IP addresses with something bad and allow things from the list of IPs we know are good.

VI. Threats to the network

VII. man in the middle

This attack is where some one manages to get in the middle of some sort of communication. A good example is if some one managed to get in the middle of communication between two people. They rewrite the messages to manipulate the people involved. Lets say for instance Bob wants to ask Sue to lunch but Greg is intercepting all the messages. So bob sends a message to Sue asking to go to lunch. Instead Greg asks Sue to send Bob some bit coin. Instead of giving Sue Bobs bit coin wallet he gives Sue hers and gets the bit coin. Its important to note that the man in the middle has a lot of power. This can also be applied to many different network protocols.

VIII. Defending against MITM attacks

There are several things that the good guys can do to defend against this tactic. For TCP we can terminate the connection every time something is sent. We could also modify the headers so that the packets that the attacker tries to write to the packet ends up filtered out by the firewall. For Mail Proxy's we can make sure that EXE files aren't sent over email. We can also look for sensitive data in emails and filter it.

IX. Vocabulary

- Zero Day Attack - An attack that has not been seen before that is new.
- Defense in Depth - The idea of using many different layers to protect your network.
- Man In the Middle Attack - A type of attack where some one intercepts traffic changes it and passes it on to its destination.