CS 373 Summer 2019

Week 6 Write Up

Kirsten Wollam

NETWORK SECURITY

Network security is an extremely important part of protecting a system. This is because the network is the outward facing front line between malicious attackers and our internal systems. It helps host-based protection by keeping dangerous and malicious actors out.

Threats

There are many types of threats that can be protected against at the network level. Here we will examine some of the main categories of attacks.

Man in the Middle

This type of attack in particular, also abbreviated as MITM, can be used for good or for evil. I a Man in the Middle set up, packets being sent are intercepted. They can then be changed or deleted by the MITM. This opens up a world of malicious options. Simple changes can totally change messages, and can direct information to unauthorized or unknown places. One way to achieve this is though Address Resolution Protocol (ARP) poisoning which uses the ARP to change the MAC address packets are sent to to the attackers so they can intercept them. MITM is often used modify TCP packets that are used for streaming. TCP is easy to hijack and insert data into the middle.

While there are significant malicious opportunities, it is also a common technique in protection strategies. They are used to scan packet traffic and protect users from intrusion. A terminating TCP proxy creates a completely new connection on the other side of the proxy to increase safety. It rewrite headers to block protocol attacks and repackages TCP packages to remove overlapping segments. HTTP proxy can be used to protect from obfuscated URLs, detect and remove malicious JavaScript or exe files, and verify destinations are not on known dangerous lists. Proxies like these are an excellent example of how MITM can be used to protect users.

Since it can be used for good or evil, strategies are needed to detect or eliminate the risks of bad MITM. HMAC, essentially an encrypted confirmation that the message is the same as original, uses public key cryptography to allow for verifying. Transport Layer Security (TLS) is industry standard and is very difficult to crack directly. This has a transaction cost though to set up the security every time so is often only used when

security is required. While these protocols are quite secure, they still only guarantee certain things cannot happen so the ways around it that need to be considered and constantly evaluated.

Recon

Attackers often want to figure out where there are vulnerabilities, find out other information that is needed for the attack like addresses, or learn about the people in the system. This reconnaissance can involve active or passive techniques including scans of the network that are often hard to see on the network as they blend in with normal traffic.

Honeynets are a good way to slow down bad actors and gather information on them at the same time. Sorting through logs for trends and problems is the main way to find these sort of attacks and can provide knowledge on what incoming attacks might look like.

Spoofing

This well-known type of attack involves the attacker masquerading as another entity entirely in order to gain access. IP and ARP spoofing can be used to initiate MITM attacks. TCP, IP, MAC address, E-Mail, HTTP fields all can be spoofed and used to get past various types of security layers.

Spoofing can be difficult to protect against. Often diligence on the part of users can prevent attacks from spoofing, but it isn't always that simple. Reverse Path Filtering is a more direct way to verify the path is valid and will drop packets that are suspicious.

Denial of Service

A Denial of Servicce (DoS) attack aims to consume resources to such an extent that it impacts the targets ability to function, sometime so bad that the service is unusable entirely. These can be easy to shut down since they come from one attack vector. To combat that, attackers have evolved to Distributed Denial of Service (DDoS) so that the threat is coming from everywhere which are much more difficult to defend against. DoS and DDoS attacks can target the network, CPU, Memory, Storage, or any other finite resources. Many motivations including Hacktivism, Financial Gain, Cyber Warfare, or Cyber Terrorism.

One way to fight against these attacks is to validate and clean traffic, check for spoofed addresses, validate protocols, block known attacks. There are centers that are made to specifically scrub data like this for clients, built to process huge amounts of data.

Defense

To fight against the many types of threats, many strategies are necessary. A good combination of detection and protection is needed, and security teams and companies combine these based on the needs of the system.

Figure 1 - Network Security Products - Network Security slide 23

These products and strategies have significant overlaps, but are usually based on some common concepts and tools. Next we will review some of these basics.

Positive Policy

Defining what you expect to happen and blocking anything else as suspicious. Gives the defender an advantage because they know what to allow and what not to. Very powerful, but makes it harder to know what the attacks are since data is not collected, and also can block too much causing good intended user to try to get around it.

Firewalls and Security Zones:

These are used to decide what is allowed to pass from one zone in a network to another. They can be used at multiple levels of the network to protect from different types of intrusion. For instance a web gateway is a proxy that reads incoming traffic and then sends it out to the destination. This allows screening to occur to block threats. Similarly an email gateway like Simple Mail Transfer Protocol filters which mail to send through to the inbox and can be set up to block malicious items or spam.

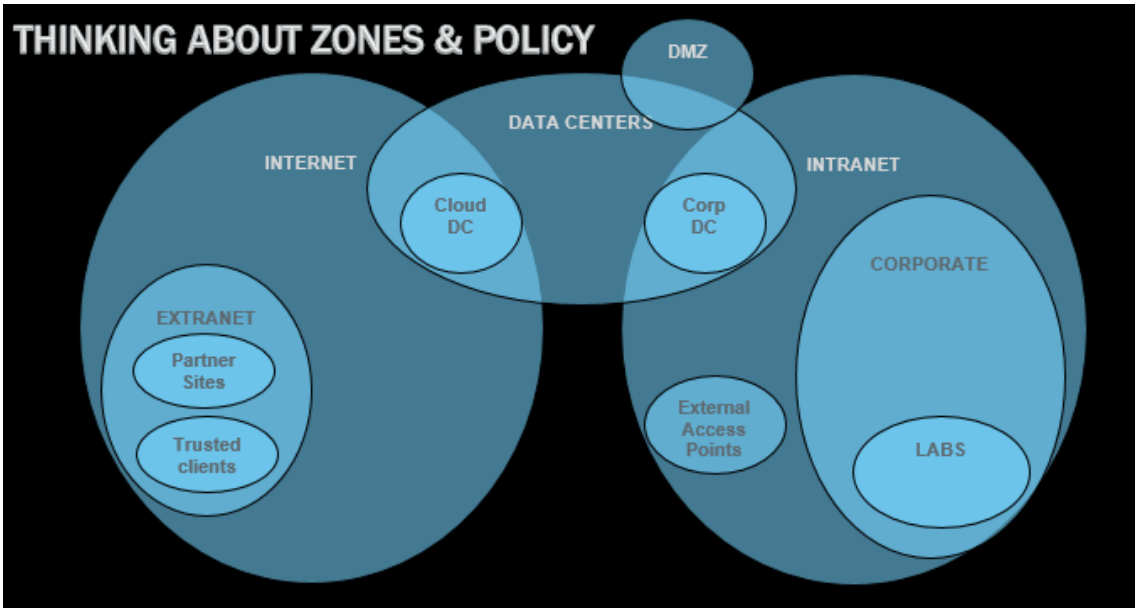

Figure 2 - Example of Network Zones - Network Security Slide 11

Defense in depth:

A good protection strategy also consists of many layers to get through to get to more important things. These layers are set up strategically. Multiple firewalls and intrusion protection systems can be used as necessary and required at the various levels.

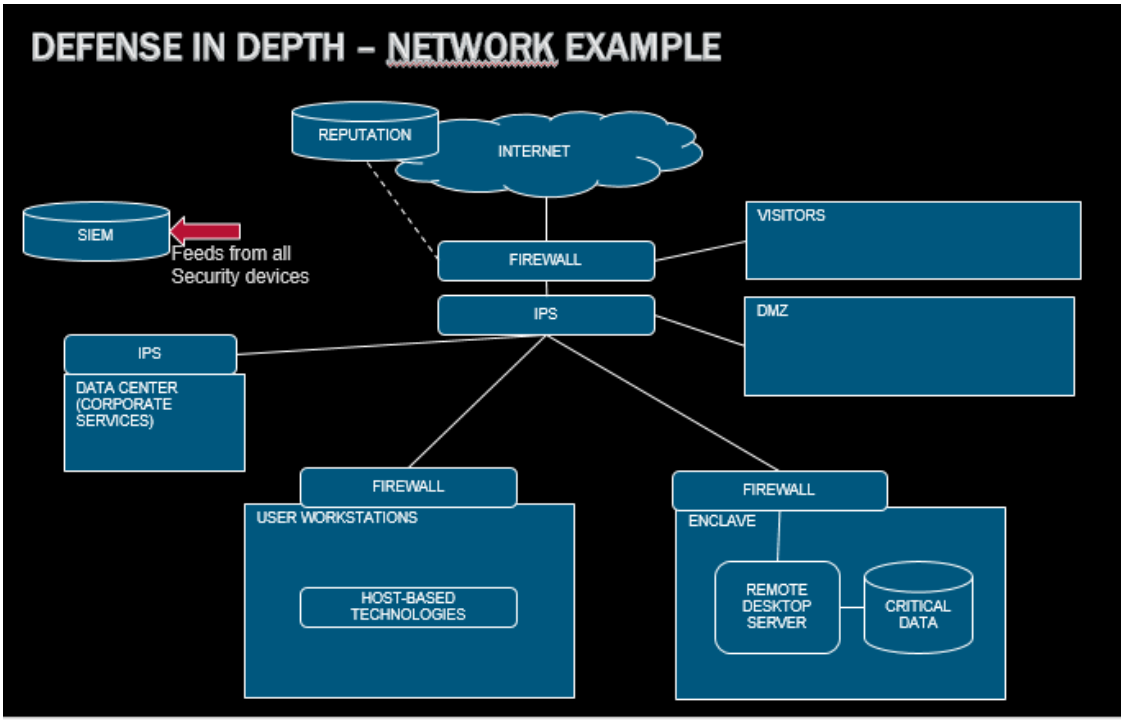

Figure 3 - Defense in Depth network example - Network Security slide 15

Intrusion Detection:

Intrusion detection and intrusion protection are tool that specifically look for threats to block. These are good at catching well known threats, but they typically cannot catch zero day attacks because they do not know about them and how to detect them. This is still very useful since there are many systems that might not be fully updated that are still vulnerable to known exploits.

Honeynet:

The idea of a honeynet is not to specifically avoid threats, but to put something out there that looks like a good target and is vulnerable as a decoy that is not actually connected to anything useful. These slow down the attacker and can also gather information about the attack. Phony content to make the attackers think it is good stuff make these work even better. They must be effective without being intrusive.

Quarantine:

This well known strategy in medicine is also easily applied to networks. It can be used to run checks before allowing people into the network or once someone is in to keep them from getting to anything important. When done well is doesn't alert the bad guys that they are stuck so they don't just come back and be even more sneaky on the next try.

Reputation:

Security certificates, black lists, mac addresses are widely used these days in network protection to confirm the reputation, good or bad. These strategies often rely on big data analysis to sort through and decide how to categorize entities. This takes significant computation, and is not foolproof, but provides an easy way to screen.

Packet Inspection

Deep inspection of packets is a good way to gain significant information about what may have transpired over a network connection. You can trace the protocol headers and signature processing. Wireshark is a tool that can record and inspect traffic. IT captures a log of all the traffic, including significant information.

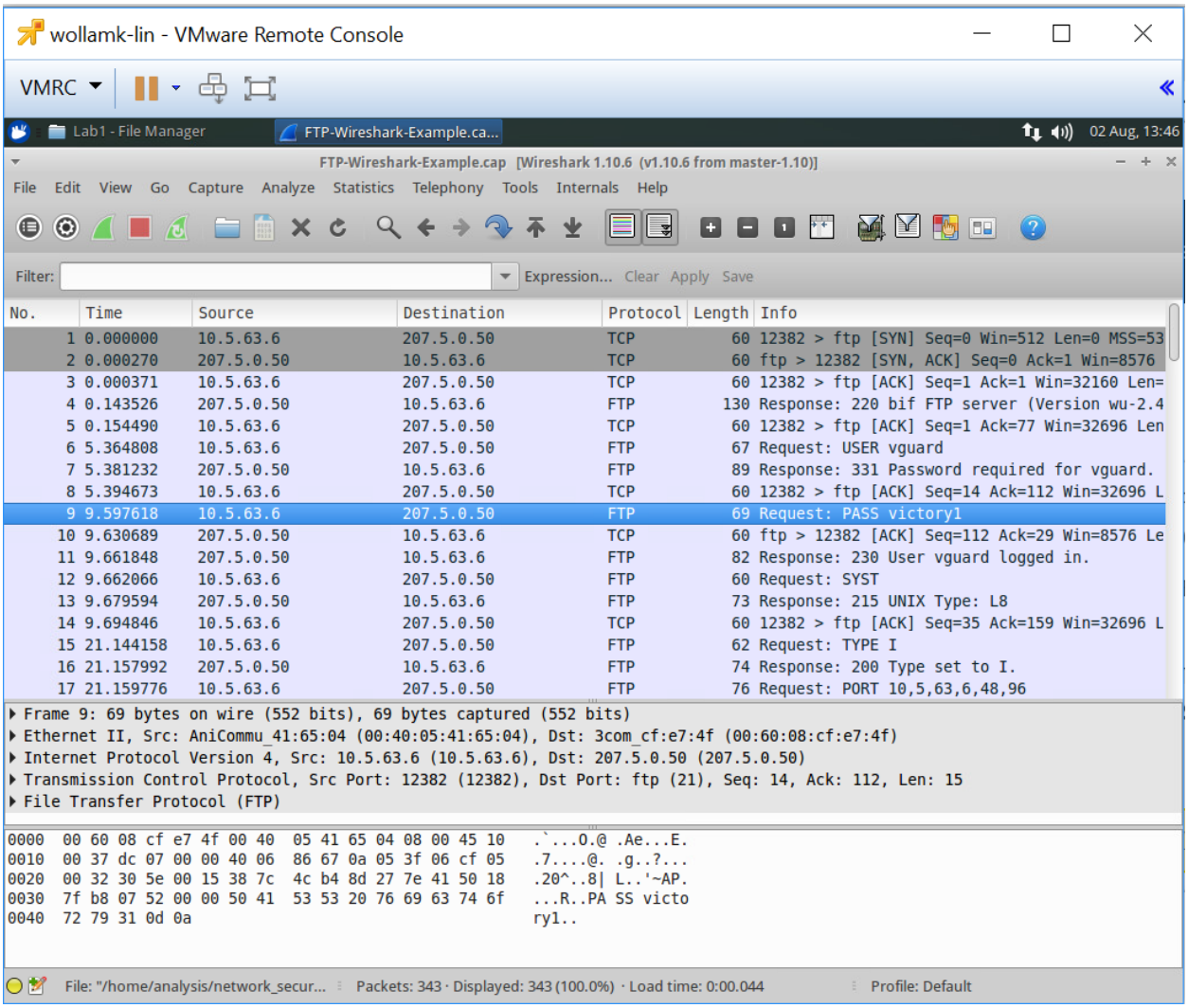

Figure 4 - Using Wireshark to view packets

The base level log shows all the packets going back and forth and includes the time, source, destination, protocol, length, and information carried. Just by clicking on a packet we can get even more additional information about that transfer. The program also has endless other ways to dig in even further, sort and analyze the information captured. One particularly interesting view is to look at the conversation streams. As seen in the image below we can follow back and forth and understand the requests each way. This can help identify malicious content for forensics. This can obviously also be used maliciously to grab things like usernames and passwords. For this reason tapping into network traffic that is not your own is very illegal.

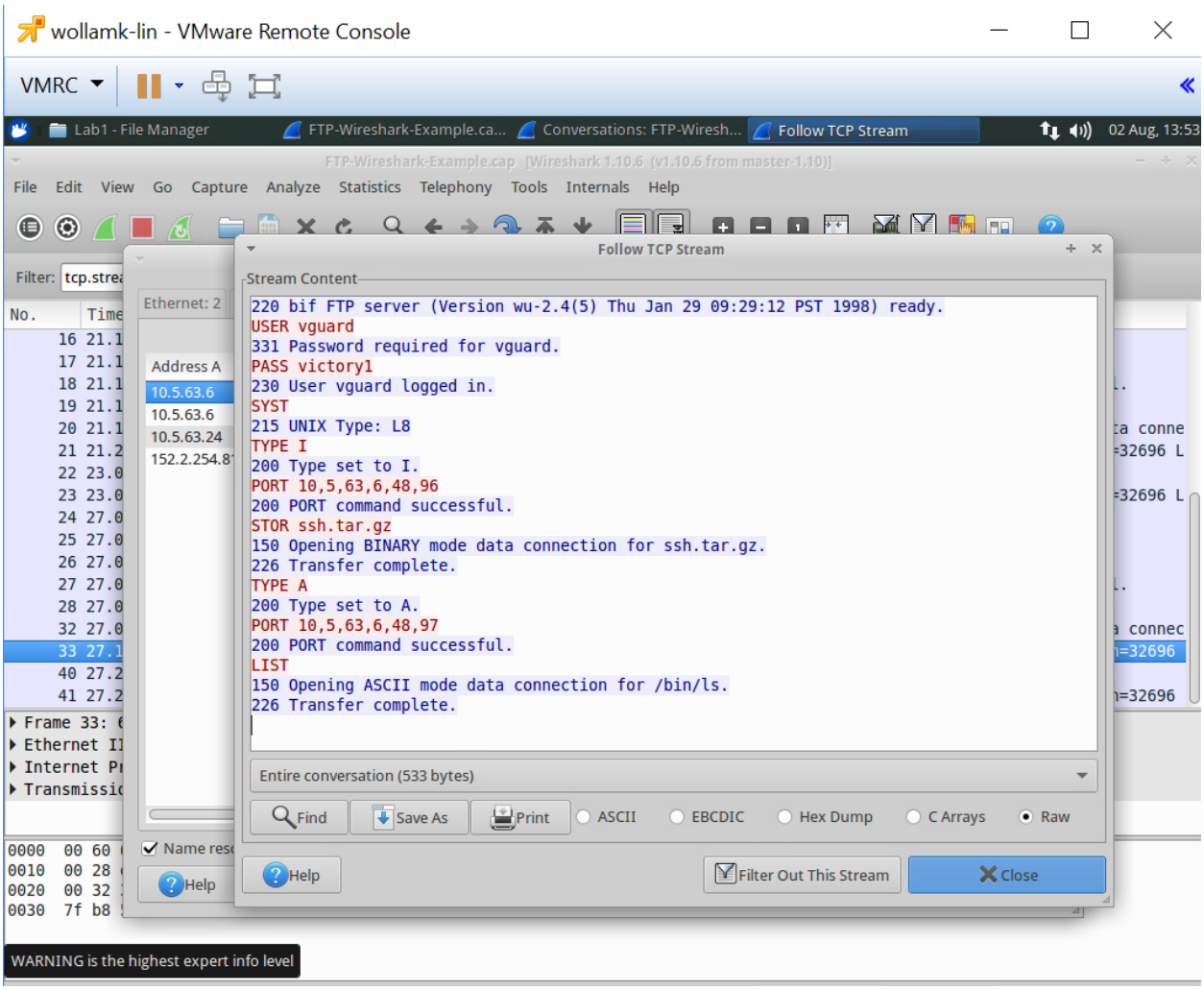

Figure 5 - view conversations in Wireshark